

UNIVERSITÀ DEGLI STUDI
SUOR ORSOLA
BENINCASA

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

www.ejplt.tatodpr.eu

ISSN: 2704-8012

2020/2

EJPLT
ISSN: 2704-8012

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

Directed by Lucilla Gatt

2020/2

UNIVERSITÀ DEGLI STUDI
SUOR ORSOLA
BENINCASA

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223



Co-founded by the
Erasmus+ Programme
of the European Union

The Journal was born in 2018 as one of the results of the European project "Training Activities to Implement the Data Protection Reform" (TAtoDPR), co-funded by the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.
From 2020, the Journal is co-funded by the Erasmus+ Programme of the European Commission within the European Project 'Jean Monnet Chair European Protection Law of Individuals in relation to New Technologies' (PROTECH) (611876-EPP-1-2019-1-IT-EPPJMO-CHAIR).

The contents of this Journal represent the views of the authors only and are their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The Issues form 2018/1 to 2020/1 were published by Giappichelli Publisher.
From issue 2020/2 the Publisher is Suor Orsola University Press.

Published by Suor Orsola University Press in December 2020
www.ejplt.tatodpr.eu

No part of this publication may be reproduced, stored, retrieved system, or transmitted, in any form or by any means, without the written permission of the publisher, nor be otherwise circulated in any form of binding or cover.

Editing
Luciana Trama

Design and printing
Flavia Soprani, Carmine Marra

© Copyright 2020 by Suor Orsola Benincasa University. All rights reserved.
The individual essays remain the intellectual properties of the contributors.

European Journal of Privacy Law & Technologies

EJPLT
ISSN: 2704-8012

EDITOR IN CHIEF/DIRECTOR
Prof. Avv. Lucilla Gatt – Università Suor Orsola Benincasa di Napoli

VICE-DIRECTOR
Prof. Avv. Ilaria A. Caggiano – Università Suor Orsola Benincasa di Napoli

ADVISOR BOARD – SCIENTIFIC COMMITTEE
Prof. Valeria Falce, Università Europea di Roma, Italy
Prof. Toni M. Jaeger-Fine, Fordham University, United States
Prof. Antonios Karaiskos, Kyoto University, Japan
Prof. Roberto Montanari, Università Suor Orsola Benincasa di Napoli, Italy
Prof. Andrew Morris, University of Loughborough, United Kingdom
Prof. Juan Pablo Murga Fernandez, Universidad de Sevilla
Prof. Alex Nunn, University of Derby, United Kingdom
Prof. Avv. Salvatore Orlando, Università La Sapienza di Roma, Italy

REFEREES
Prof. Carlos Antonio Agurto Gonzáles, Universidad Nacional Mayor de San Marcos, Peru
Prof. Avv. Giuseppina Capaldo, Università La Sapienza di Roma, Italy
Prof. Cristina Caricato, Università di Roma Sapienza
Prof. Roberto Carleo, Università degli Studi di Napoli Parthenope, Italy
Prof. Georges Cavalier, Université de Lyon, France
Prof. Carlos de Cores Helguera, Universidad CLAEH del Uruguay, Uruguay
Prof. Manuel Espejo Lerdo de Tejada, Universidad de Sevilla, Spain
Prof. Giovanni Iorio, Università degli Studi di Milano Bicocca, Italy
Prof. Arndt Künnecke, Hochschule des Bundes für öffentliche Verwaltung, Germany
Prof. Martin Maguire, University of Loughborough, United Kingdom
Prof. Giovanni Martini, Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Alessia Mignozzi, Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Roberta Montinaro, Università degli Studi di Napoli l'Orientale, Italy
Prof. Salvatore Monticelli, Università di Foggia, Italy
Prof. Cinzia Motti, Università di Foggia, Italy
Prof. Nora Ni Loideain, Institute of Advanced Legal Studies of London, United Kingdom
Prof. Taiwo Oriola, University of Derby, United Kingdom
Prof. Francesco Rossi, Università degli Studi di Napoli Federico II, Italy
Prof. Maria A. Scagliusi, Universidad de Sevilla, Spain
Prof. Avv. Laura Valle, Libera Università di Bolzano, Italy

European Journal of Privacy Law & Technologies

EJPLT
ISSN: 2704-8012

COORDINATOR OF THE EDITORIAL BOARD

Ph.D. Avv. Maria Cristina Gaeta, Università degli Studi Suor Orsola Benincasa, Italy

MEMBERS OF THE EDITORIAL BOARD

Prof. Sara Lorenzo Cabrera, Universidad de La Laguna, Spain
Prof. Manuel Pereiro Càrceles, University of Valencia, Spain
Prof. Maria Ioannidou, Queen Mary University of London, United Kingdom
Prof. David T. Karamanukyan, Siberian Law University, Russia
Prof. Avv. Alessandra Sardu, Università Suor Orsola Benincasa di Napoli, Italy
Prof. Hakeem Yusuf, University of Derby, United Kingdom
Ph.D. Avv. Andrea D'Alessio, Università degli Studi di Teramo, Italy
Ph.D. Avv. Caterina del Federico, Alma Mater Studiorum Università di Bologna, Italy
Ph.D. Matteo Fermeglia, Hasselt University, Belgium
Ph.D. Avv. Paola Grimaldi, Università degli Studi di Napoli Federico II, Italy
Ph.D. Avv. Anita Mollo, Università Suor Orsola Benincasa di Napoli, Italy
Ph.D. Avv. Michael William Monterossi, Universität Luzern, Switzerland
Ph.D. Sara Saleri, Re:Lab, Italy
Ph.D (c) Avv. Livia Aulino, Università Suor Orsola Benincasa di Napoli, Italy
Ph.D (c) Noel Armas Castilla, Universidad de Sevilla, Spain
Ph.D. (c) Emanuele Garzia, Università Suor Orsola Benincasa di Napoli, Italy
Ph.D (c) Avv. Valeria Manzo, Università degli Studi della Campania Luigi Vanvitelli, Italy
Ph.D (c) Emiliano Troisi, Università Suor Orsola Benincasa di Napoli, Italy
Ph.D (c) Hans Steege, Gottfried Wilhelm Leibniz Universität Hannover Volkswagen AG, Germany
Avv. Delia Boscia, Università Suor Orsola Benincasa di Napoli, Italy
Avv. Flora Nurcato, Università Suor Orsola Benincasa di Napoli, Italy
Avv. Ranieri Razzante, Università degli Studi di Bologna, Italy
Avv. Chiara Vitagliano, Università Suor Orsola Benincasa di Napoli, Italy
Dr. Alessandra Fabrocini, Università Suor Orsola Benincasa di Napoli, Italy
Dr. Simona Latte, Università Suor Orsola Benincasa di Napoli, Italy

pp.

PASQUALE STANZIONE - *Data protection and vulnerability.* 9

Section I: **Articles**

LAURA VALLE - *Cookies e tutela dei dati personali tra protezione dei diritti della persona e tutela del consumatore*
16

ANDREA D'ALESSIO – *Online platforms: new vulnerabilities to be addressed in the European legal framework. Platform to business user relations.*
36

ROBERTA MONTINARO – *Online platforms: new vulnerabilities to be addressed in the European legal framework. Platform to consumer relations.*
53

VIOLA CAPPELLI - *The legal qualification of collaborative platforms offering composite services. What consequences for consumer protection?*
65

SILVIA MARTINELLI - *The vulnerable business user: The asymmetric relationship between the business user and the platform.*
82

SEBASTIÃO BARROS VALE - *The Omnibus Directive and online price personalization: A mere duty to inform?*
92

MARIA CRISTINA GAETA - *Smart toys and minors' protection in the context of the Internet of Everything.*
118

CHIARA SARTORIS – *Minors's data protection between e-learning and social network platforms.*
138

ARNDT KÜNNECKE - *Distance teaching in times of corona – from zero to hero? Experiences and best practices of a university lecturer trying to create a student-centred distance teaching approach.*
148

ANTONINA ASTONE - *Capitalism of digital surveillance and digital disintermediation in the era of the pandemic.*
165

ALDO IANNOTTI DELLA VALLE - *The (in)adequacy of the law to new technologies: The example of the Google/CNIL and Facebook cases before the Court of Justice of the European Union* 172

NICOLETA CHERCIU AND TEODOR CHIRVASE - *Non-personal data processing – why should we take it personally?* 183

PAOLA GRIMALDI - *Robots, unwearable profiling and protection of vulnerable users.* 193

ANTONELLA CORRENTI - *Online market, big data and privacy protection.* 200

DMITRY E. BOGDANOV - *Model of liability for harm caused to the patient by the use of bioprinting technologies: View into the future.* 213

FABRIZIA ROSA - *The use of IT tools and artificial intelligence in the health sector: The patient as a vulnerable subject.* 224

MIRKO FORTI - *Migrants and refugees in the cyberspace environment: Privacy concerns in the european approach.* 241

LIVIA AULINO, MARCEL SAAGER, MARIE-CHRISTIN HARRE AND LEONARDO ESPINDOLA - *Consideration of privacy aspects in the area of highly automated driving. An intention recognition use case.* 252

ANNA IRENE CESARANO - *Autonomous driving: An exploratory investigation on public perception.* 265

LIVIA AULINO - *Human machine interaction and legal information in the autonomous vehicles: The opportunity of the legal design.* 275

ANNA ANITA MOLLO - *La soggettività giuridica degli esseri nonumani: gli animali.* 291

MASSIMILIANO CICORIA - *L'io, l'altro e il bilanciamento degli interessi nella artificial intelligence* 303

Section II: **Focus papers**

VALERIA MANZO - *Child protection on social networks in the era of Covid-19 confinement.* 319

PAOLA GRIMALDI - *Energy and sustainability between ecology of law, green law and nature rights* 328

SERGIO GUIDA - *Un framework per il contact tracing in italia tra esigenze scientifiche, possibilità tecnologiche e rispetto di diritti e libertà individuali in termini di data protection.* 332

SIMONA LATTE - *Immuni: inquadramento e prime considerazioni ad un mese dal via.* 362

List of authors 374

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Data Protection and vulnerability

PASQUALE STANZIONE
President of the Italian Data Protection Authority

Abstract

This contribution describes the evolution of the right to privacy from the traditional right to be let alone to data protection, enshrined as an autonomous right in the Charter of Fundamental Rights of the European Union. While illustrating the most innovative features of this right, the author also emphasizes that data protection represents an essential guarantee for freedom, equality and dignity with respect to vulnerabilities: both traditional ones and those induced by new technologies.

Keywords: data protection - dignity - equality - habeas data - identity – labeling - new technologies - right to be let alone - vulnerability.

The title of my speech underlines an essential idea: the awareness of how today new technologies expose us to new vulnerabilities and amplify the more 'traditional ones'.

If in the early twentieth century the 'domain of technology' was considered a distinctive feature of the post-modern age, it characterizes, even more, our times, in which technology risks losing its instrumental nature to become an aim in itself, making a human being no more its dominus but subordinate to itself. This happens essentially for an intrinsic characteristic of new technologies: the transforming power, the ability to develop new meanings of the reality.

The news hierarchy decided by algorithms, the selective power of indexing that shows only some contents and not others, are a paradigmatic example of how new technologies condition the very formative process of our beliefs, shaping public opinion and undermining the individual self-determination.

So it's up to the law to restore that human being centrality, which alone is a guarantee of a harmonious relationship with the technology and, at the same time, consolidates the personalist approach on which our Constitution and the EU system are based, whose activities place the individual at their heart, as stated by the preamble of the Charter of Fundamental Rights of the European Union.

This approach - both progressive, democratic and personalist -has made it possible to govern the relationship between individual and technology according to the evolution of the right to privacy in Europe in all its complexity, from traditional right to be let alone to data protection. As stated by the Council of Europe Convention n.108/1981, this right has to be read as a protection of individuals with regard to automatic processing of personal data. Data protection will acquire 'constitutional' rank with the Charter of Fundamental Rights of the European Union, as *habeas data:* equivalent, in the digital society, of what *habeas corpus* has represented since the Magna Carta; as the main prerequisite of immunity from power, it is promoted by the State, the market or technology.

Significant was the assonance with the Riley v. California ruling of 2014, by which the American Supreme Court extended the traditional guarantees provided for measures restricting personal freedom to the search of cell phones. The connection established between physicality and the electronic body is here much more than symbolic: the traditional guarantees granted to the h*abeas corpus* are extended to *habeas*

data, according to that evolutionary line that has made privacy a prerequisite of freedom and democracy together.

In Europe, however, the path of privacy has also marked an essential turning key in terms of values, emancipating this right from the dominical dimension of traditional bourgeois prerogative (right to be let alone), in order to assert itself as a means of protecting the socially weaker fringes from the abuse of a power that is primarily informative. This 'enrichment' of the original nucleus of the right with more modern demands was made possible by the conjunction, borrowed from the European system, of the American idea of constitutional privacy with the more continental one of guaranteeing social dignity.

Thus, on the one hand, the idea of informative self-determination has developed as a new expression of freedom of the individual in the construction of his/her own identity.

On the other hand, in its not only recent evolution, privacy has developed in all its potentiality the component linked to dignity, enshrined by the post-war Constitutions and, in particular, by those (Italian and especially German) of the countries where totalitarian regimes had carried out the worst violations of the 'right to have rights'.

This idea would have deeply permeated the jurisprudential, but also the legislative reading of data protection, according to a line that from the guarantees of freedom of the worker established by the 1970 Statute, would then have reached the anti-discrimination component of privacy, as a factor of protection of minorities or individuals particularly vulnerable to risks of stigmatization.

With the introduction of a dynamic protection, with a strong publicistic vocation, also based on the powers of intervention and control of the data subject, what had traditionally been conceived as *jus solitudinis*, intangibility of the private sphere from undue external interference, has thus been enriched with a new content and, in comparison with a reality so deeply affected by new technologies, has become a pre-condition for equality and for the exercise of fundamental rights.

In this sense, the right to data protection develops, to the end, the American idea of privacy as freedom of self-determination, a counter-majoritarian defence 'of the undecidable' sphere from primarily State interference, which has allowed, for example, in the USA, the right to contraception and abortion to be rooted on the Fourth and Fifth amendments (Griswold vs. Connecticut 1965, Roe vs. Wade , 1973), and in Europe on art. 8 ECHR to envisage the right to death with dignity [(Pretty v. UK 2002], to make use of assisted procreation (Costa and Pavan v. Italy, 2012) or the right of the born to seek their own origins, although compatible with the choice of maternal anonymity (Godelli v. Italy, 2012).

However, in the European reading, the dignity component has also made it possible to develop the social dimension of privacy (increasingly characterized, in the meantime, as protection of the individual with regard to the processing of his/her data) as the right to freely live out one's individuality also in the social dimension, protected from discriminatory risks or social stigmatization (ECtHR, Delfi AS v. Estonia, Sidabras v. Lithuania, 2015).

For this reason, since Convention 108 and, shortly afterwards, with the directive 95/46, enhanced protection has been granted to sensitive data (and in particular to those expressing an associative choice), demonstrating that privacy, far from encouraging isolation, is instead functional to freely establish strong social ties and also, where appropriate, connoted from an ideal point of view. Sensitive data were and are protected, in fact, to guarantee not their secrecy but their maximum public disclosure, without thereby exposing the data subject to discrimination. The anti-discrimination function of data protection (and,

above all, of sensitive data) would then prove, in the years to come, to be an extraordinary guarantee of equality, in a society increasingly prone to labelling.

It is significant, in this sense, that the Court of Cassation, in the case of sick children, has decided to extend the enhanced protection granted to their health data to their parents as well, because of the discriminatory potential related to information on the condition of discomfort and particular vulnerability, typical of those who are burdened with the care of children suffering from diseases (Cass., n. 16816/2018).

As is also relevant the expected subtraction of the disclosure obligations of data relating to grants, from which the socio-economic condition of the beneficiary can be inferred (Article 26, paragraph 4, Legislative Decree 33/2013).

This anti-discrimination vocation has represented the center of gravity around which the gradual transition from traditional privacy to data protection has emerged, progressively establishing itself as a constituent element of a new form of citizenship able to strengthen the conditions for citizens' participation in collective life, thus favouring sociality also -and above all- for those who would have feared its repercussions on the individual sphere, because of their own subjective conditions. Therefore - according to the scheme for which '*remedies precede rights*' - that fundamental passage 'from secrecy to control' was outlined, made possible also by a jurisprudence of the European Court of Justice that emphasized the properly constitutional dimension of this right.

Despite the protection of data was born, in fact, as functional to the development of the internal market, the scope of the directive has gradually reversed the terms of the relationship**,** enhancing the protection of that right 'to freedom' which, according to the Court, should be given precedence over the mere interest of controllers to increased profits (C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [2014]). And if in this case the Court has recognized a real *Drittwirkung* to the right to data protection, with regard to a private subject such as Google, elsewhere it has gone so far as to establish the direct applicability of the proportionality principle (C-139/01 *Österreichischer Rundfunk and Others* [2003].). A strong reading of this principle - heterointegrative of reasonableness principle – has allowed our Constitutional Court to outline a democratically sustainable balance with respect to the relationship between data protection and administrative transparency (Const. Court, n. 20 of 2019). Thanks to the reconsideration, in a personalist key, of this relationship, it has in fact been possible to bring the discipline of administrative transparency back to its democratic function of 'governing public affairs in public', counteracting the paradoxical effect of opacity from information excess, due to the unreasonable extension of publicity obligations.

But the social function of data protection has also proved to be decisive with respect to the 'structural', almost ontological vulnerability that characterizes the position of the individual about the increasingly pervasive private powers, exercised with the pretension of inscribing the code of life and society in the general contract conditions.

Here I'm using the term 'vulnerability' in the meaning in which it can be connected, for example, also to the consumer, that is to say with reference to general categories connoted due not so much to specific subjective as to relational characteristics, i.e. derived from the relationship in whose context they are considered. Here lies the transition from the abstract, 'disembodied' subject, to the person, in the peculiarity of his/her condition (*homme situé*).

Precisely this passage has allowed a new approach to vulnerability, which is a paradoxical notion, because it is both a prerequisite and an effect of human autonomy. But it is also a complex notion , because it is universal - all human beings are vulnerable -

individual - since it does not affect all people in the same way -; potential - possible, but not certain realization of a risk -; relational and contextual - we are vulnerable in a given context: moreover, it is society that makes individuals vulnerable, not the contrary -; finally, reversible - and in fact with appropriate individual and social measures it is possible to reverse this condition.

On the basis of these elements, we can outline a basic notion of 'vulnerability' as a common connotation of the human condition (a sign of existence, for Simon Weil), next to which it can be seen the variability of the situations in which it is declined: conditions due to age, gender, health and other discriminating factors. One of these conditions may, however, also be the relationship, legal and socio-economic, structurally asymmetrical, of which the subject is a weak part: so for the consumer or the user of digital platforms.

Concerning the latter subjective category, data protection discipline offers some decisive guarantees to rebalance its conditions of vulnerability, at least partially curbing the irresponsible power of web titans.

Through the application - possible, under the GDPR, without further requirements - of the European law to extra-European controllers, it has in fact been possible to impose limits on the irrepressible collection of data, assimilated to mere currency to be deducted in contract, with the risk of monetization of privacy, which today represents the real democratic issue.

On this ground, the Italian Data Protection Authority has promoted a debate within the European Data Protection Board, in the awareness of how this issue represents an essential matter in the evolution of data protection law. On the one hand, in fact, the *zero price economy* has made the 'services versus data' negotiation scheme an ordinary practice; on the other hand, admitting the possibility of remuneration for consent risks leading to the creation of digital sub-proletariat, i.e. social strata likely to surrender, with their data, the essential core of their freedom.

On this 'slippery slope' is at stake, perhaps more than in any other field, the European identity as a 'Community of law' founded on the synergy between freedom, dignity, equality, as essential safeguards that no reason of State or, much less, the market can violate. And in this sense, data protection may represent an extraordinary barrier to the risk of refeudalization of social relations and reconstitution of census-type discrimination even among users of the internet, whose inclusive and democratic vocation risks succumbing under the weight of surveillance capitalism.

With respect to the condition of particular vulnerability of the minor, then, the Italian legislator has given the Italian Data Protection Authority a central role in the fight against cyberbullying, assigning him the power to decide on instances for the removal of illegal/harmful content. This is a forward-looking provision, aware of how children today can represent the elective 'victims', at the hands of their own peers, of a misuse of the internet, where their fragility is amplified also due to the reduced perception of the terribly concrete impact of every gesture, of every word, every image posted on social networks.

But the context in which data protection can represent a fundamental defence for the individual with regard to new and subtle forms of discrimination is that of artificial intelligence and algorithmic decision making, to which decisive and far from neutral choices are increasingly being delegated, for private and public life: from medical diagnosis to 'predictive' police, from the assignment of teaching locations even to the assessment of the adoptive suitability of couples (as in Florida).

Moreover, not even what has traditionally been considered the last bastion of human assessment, namely judicial (in particular criminal) process, seems immune from the

tendency to mechanize decisions, with effects often much more discriminatory than those of the worst human decision.

An algorithm used in some American courts for the prognosis of criminal recidivism has been proved, for example, inclined to grant a higher score to African-Americans, of course in the absence of any criminological reason, but only on the basis of the statistics taken as a reference photographing a penitentiary and judicial condition not really representative of the phenomenon.

The result to be drawn from the use of technologies that should ensure maximum impartiality is likely then to be, paradoxically, more discriminatory than the " human, too human 'rationality', at least whenever the algorithms reflect the pre-comprehensions of those who design them or are 'trained' with data that are not representative of actual reality, in all its complexity.

From this point of view, both the GDPR and the law enforcement directive (n. 2016/680) provide some essential guarantees which are increasingly being used in case law to establish an embryonic legal status for artificial intelligence.

In fact, not only does the Regulation subject the admissibility of fully automated decisions based on 'special categories' of personal data to particularly restrictive conditions, but in any case recognizes the right to an explanation of the underlying logic, to challenge it and to obtain human intervention in the automated process, precisely to correct any *bia*s that might otherwise produce detrimental effects.

These reinforced obligations of algorithmic transparency are, however, particularly relevant precisely because they allow to overcome, at least in part, the opacity of such processings, which really makes such decision-making processes the new *arcana. imperii.*

A further guarantee of a preventive nature then derives from the necessary subjection of automated decisions to impact-privacy assessments: an institution which, precisely because of its effectiveness, has been proposed to enhance in a broader perspective, allowing the assessment of similar processings' impact not only on data protection but, more generally, on rights and freedoms, given the natural interrelation between data protection, dignity and other fundamental rights. Widening its spectrum, the impact assessment would become a PESIA: privacy, ethical and social impact assessment*:* a prognosis of the ethical and societal impact of processing, conducted according to the parameters of respect for fundamental rights and anti-discrimination protection as well as the right to data protection.

The requirements set out in the GDPR were enhanced by the Council of State which, in the case of teachers' algorithm, considered the software to be a 'digital administrative act', to be subject to full jurisdiction guarantees according to an 'enhanced declination of the transparency principle ', as well as to the prohibition of the exclusive algorithmic decision and to the equality and non-discrimination principle.

The risk of discriminatory use of algorithmic decisions, all the more so if functional to the exercise of coercive power is, moreover, the subject of particular attention under Directive 2016/680 and Legislative Decree 51/18 that transposed it. If, in fact, the former has enshrined an express prohibition of automated decisions based on special categories of data, which induce discrimination, the latter has been granted criminal protection, in an aggravated form, in awareness of the risk of a combination of investigative power and the increasingly strong one of technology, especially for the most vulnerable subjects.

The racial profiling sometimes practiced in the aftermath of September 11th. by law enforcement officials, targeting individuals for suspicion of crime based on the individual's race, ethnicity, religion or national origin, comes to mind. If these pre-comprehensions are added to the computing power, the pervasiveness of digital investigations and the profiling capacity of the algorithms, the risk of further deeper and more subtle discrimination against

minorities or of those perceived as 'different' is greatly aggravated.

It is no coincidence that the European Union is investing a great deal of its identity building in this area, also in its relationship with the USA, as well as demonstrated by Schrems jurisprudence and the personalist vocation already underlying the Ventotene manifesto is taking on new horizons.

As President of the Italian Data Protection Authority, at the beginning of a mandate that will go on for important years, I can already indicate, as a priority objective, the protection of vulnerable subjects such as minors, migrants, sick people, inmates in prison, or in any case belonging to minorities; of all those whose fragility - by nature or circumstance - risks making them really 'naked' in the face of power.

It is precisely on this very delicate ground that data protection will express its profound sense, as a precondition of any other right or freedom; a prerequisite for a society of dignity.

SECTION I
ARTICLES

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Cookie e tutela dei dati personali tra protezione dei diritti della persona e tutela del consumatore

LAURA VALLE
Associate Professor of Private Law at the Free University of Bolzano

Abstract

I cookie sono utilizzati in maniera generalizzata dagli operatori che gestiscono siti internet, sia con finalità sia di tipo tecnico e funzionale ma anche con finalità di analisi delle visite che ricevono sui loro siti internet e per finalità di marketing e di profilazione degli utenti. Si riscontra oggi un uso piuttosto aggressivo di questo strumento da parte degli operatori e una diffusa mancanza di rispetto della disciplina normativa data per il trattamento dei dati personali degli utenti. Recentemente si sono avute più importanti decisioni giurisprudenziali e delle autorità garanti dei dati personali in materia, che hanno chiarito alcuni profili fondamentali delle regole normative applicabili all'uso dei cookies. Sono intervenute anche diverse linee guida da parte delle autorità nazionali di protezione dei dati personali e anche ad opera dell'Editorial Data Protection Board (EDPB). Nonostante le une e le altre rappresentino degli importanti punti di riferimento, alcune riflessioni e qualche indice in via di emersione suggeriscono di attendersi per il prossimo futuro possibili evoluzioni.

Keywords: cookie - privacy - data protection - dati personali.

Summary: Introduzione. – 1. Il quadro normativo del trattamento dei dati personali relativo all'utilizzo dei *cookie* e la trasposizione della disciplina normativa in segni grafici. – 2. Le pratiche adottate dagli operatori nell'utilizzazione dei *cookie*. – 3. Interpretazioni recenti della disciplina del trattamento dei dati personali in relazione all'uso dei *cookie*. Azioni e rimedi per il mancato rispetto dei diritti dell'interessato. – 4. Recenti decisioni sull'impiego dei *cookie* ed evoluzione delle pratiche diffuse sul mercato. – 5. Uso dei *cookie* e disciplina di tutela del consumatore. 6. Uso dei *cookie* e tutela dei diritti fondamentali della persona diversi dal diritto alla protezione dei dati personali. – Conclusioni.

Introduzione.

Nella navigazione quotidiana su internet si sperimenta il ricorso generalizzato da parte degli operatori che gestiscono siti[1] *online* all'utilizzo dei *cookie,* ossia di «file di piccole dimensioni che un *web server* immette nei computer e nei dispositivi durante la navigazione» e che come dei marcatori elettronici consentono di riconoscere i dispositivi utilizzati per la navigazione e, come conseguenza, la persona dell'utente[2]. I *cookie* vengono impiegati per

[1] Si utilizza un linguaggio colloquiale, seguendo il linguaggio del d.lgs. n. 70/2003 si adotterebbe invece l'espressione di "fornitori di servizi della società dell'informazione".

[2] «La ragione originaria dell'adozione del sistema dei *cookie,* introdotti per la prima volta dal *browser* Netscape a metà degli anni Novanta, era di natura commerciale» in quanto senza di essi non era possibile identificare un utente durante la navigazione. Così che prima della loro introduzione all'uso non era possibile ad esempio selezionare un prodotto da acquistare in un sito di *e-commerce* per poi ritrovarlo nel carrello in quanto la rete non consentiva di seguire un singolo utente durante la navigazione e di identificarlo come il medesimo utente che aveva selezionato il prodotto e che accedeva al carrello per procedere all'acquisto nella pagina successiva. «Grazie al sistema di tracciamento tramite *cookies* è stato possibile realizzare una serie di funzioni durante la navigazione, frutto della memorizzazione delle azioni e delle preferenze dell'utente (ad esempio, le impostazioni di visualizzazione o la lingua preferita)». In via generale va tenuto presente che - come si vedrà qui di seguito nel testo - i *cookie* sono uno degli strumenti più efficaci per identificare gli utenti e hanno contribuito in modo

raccogliere (trattare[3]) numerosi dati personali[4] degli utenti, che vanno dagli identificativi personali, ai dati sulla loro localizzazione[5], sulle loro preferenze di navigazione e di acquisto, solo per citarne alcuni. I dati personali dell'utente vengono trattati dagli operatori per più finalità: dal rendere possibile la medesima navigazione sul sito, alla profilazione delle abitudini di navigazione dell'utente.

I *cookie* più diffusamente impiegati vengono classificati e denominati, per la serie di dati che raccolgono e per gli scopi per cui tali dati vengono raccolti, come *cookie* necessari, funzionali, analitici, di profilazione. I *cookie* necessari trattano i dati dell'utente che sono necessari allo scopo di rendere possibile in senso tecnico la navigazione sul sito, i *cookie* funzionali trattano dati diretti a consentire l'utilizzazione di determinate funzionalità del sito e la loro memorizzazione come ad esempio la lingua utilizzata dall'utente per la navigazione, i *cookie* analitici sono diretti ad analizzare i dati di navigazione degli utenti, i *cookie* di profilazione a trarre informazioni sulle preferenze degli utenti e vengono solitamente utilizzati dalle imprese per ricerche di mercato e per finalità di *marketing*[6]. Ricorre poi quasi sempre nella raccolta dei dati personali degli utenti attraverso i *cookie* la cessione di tali dati a soggetti terzi[7], che si qualifica come un ulteriore trattamento dei dati[8]. Se in alcuni casi si

---

determinante a favorire la possibilità di monitorare e tracciare chi naviga in rete. SMORTO, in QUARTA e SMORTO, *Diritto privato e dei mercati digitali*, Milano, Le Monnier Università, 2020, p. 55.

[3] Il Reg. 2016/679 all'art. 4 n. 2 definisce il "trattamento" dei dati personali come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione». Nel caso dell'impiego di *cookie* i dati personali vengono sottoposti a più tipologie di trattamento, anche in linea con i diversi dati trattati e con lo scopo per il quale vengono trattati.

[4] La definizione di "dato personale" si trova all'art. 4 n. 1 del Reg. 2016/679 secondo la quale è dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

[5] C.d. geolocalizzazione, cioè la posizione geografica in cui si trova una determinata persona o un determinato oggetto nel mondo reale.

[6] Segnala l'Allegato 1 alla Consultazione sulle "Linee guida sull'utilizzo dei *cookie* e di altri strumenti di tracciamento" del nostro Garante della *privacy* del novembre 2020, p. 4 – su cui si dirà più ampiamente più avanti - che la classificazione dei *cookie*, in base alla *ratio* della disciplina normativa e alle esigenze di tutela della persona, si basa in definitiva su due macrocategorie: i *cookie* tecnici, utilizzati al solo fine di «effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore dei un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio» (art. 122, comma 1° cod. *privacy*); e i *cookie* di profilazione, utilizzati per ricondurre a determinati soggetti specifiche azioni o schemi comportamentali ricorrenti in modo da poter loro inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nel corso della navigazione in rete. Tale intervento del Garante indica una certa propensione a fare rientrare i *cookie* analitici tra i *cookie* tecnici, purché sia preclusa la possibilità di pervenire, mediante il loro utilizzo, all'individuazione dell'interessato (c.d. *single out*), ciò che equivale ad impedire l'impiego di *cookie* analitici che siano identificatori diretti ed univoci. Tuttavia, si riferisce che ad oggi non esiste un sistema universalmente accettato che consenta univocamente di distinguere i cookie tecnici, dai *cookie* analitici e dai *cookie* di profilazione, se non basandosi sulle indicazioni rese dal titolare della *privacy policy* (pp. 11-12). Questa linea è stata confermata nel Provvedimento definitivo adottato dal Garante il 10 giugno 2021 (n. 231) – su cui *infra*, par. 3 - che ha classificato tra i *cookie* tecnici i *cookie* analitici anonimizzati. Più severa nel richiedere il consenso rispetto ai *cookie* analitici la *Data Protection Commission* irlandese nella *Guidance Note: Cookies and other tracking technologies*, aprile 2020, pp. 7-8.

[7] Si distinguono infatti i *first party cookie* dai *third parties cookie*, su tali due serie di *cookie* si può v. Cfr. ROSSI CHAUVENET e STEFANINI, *Internet e* privacy*: il recepimento in Italia della direttiva sulla* cookie law, in *Resp. civ. prev.*, 2012, pp. 1810.

[8] Si v. *supra*, nota 3, la definizione di trattamento dei dati data dall'art. 4 del Reg. 2016/679.

tratta di soggetti terzi che gestiscono il trattamento dei dati per conto dell'impresa loro cliente fornendole dei servizi, tantissime volte la cessione dei dati a soggetti terzi è finalizzata al loro utilizzo per scopi pubblicitari che consistono nell'indirizzare all'utente presso il quale sono stati raccolti i dati personali messaggi pubblicitari in linea con i suoi interessi[9]. I *cookie* si dividono poi in due macrocategorie in ragione della durata della loro permanenza nella memoria del computer dell'utente, a seconda che si autoeliminino al momento della chiusura del *browser* e si tratti quindi di *cookie* «di sessione», oppure permangano nella memoria del computer per più tempo e si dicano perciò «persistenti» [10].

Da tempo il trattamento dei dati personali e quindi anche il trattamento dei dati attraverso i *cookie* è regolato dalla legge, prima dalla dir. 95/46 Ue, attuata nel nostro Paese con la l.n. 675/96 che è stata poi assorbita nel codice della privacy del 2003, e successivamente dal Reg. 2016/679 Ue (detto anche GDPR, acronimo di *General Data Protection Regulation*) che ha abrogato la precedente direttiva. Una disciplina più specifica è quella contenuta nella dir. 2009/136 Ue[11] che ha portato ad una modifica dell'art. 5.3 della dir. 2002/58 e quindi dell'art. 122 cod. privacy con riguardo all'«archiviazione di informazioni» e all'«accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente». Sull'utilizzo dei *cookie* sono intervenuti anche più pareri del *Working Group Art. 29*[12]: il parere 2/2010 sulla pubblicità comportamentale *online*, il parere 4/2012 sull'esenzione dal consenso per l'uso dei *cookie*, e il documento di lavoro 2/2013 che fornisce una guida per il consenso all'uso dei *cookie*[13]. Successivamente si è occupato di *cookie* il nostro Garante della *privacy* con un suo Provvedimento del 2014[14], che è tornato sulla materia di recente avendo aperto una Consultazione nel novembre 2020 che si chiusa con l'adozione

[9] Il tracciamento degli utenti durante la navigazione in rete consente la creazione di profili che vengono successivamente utilizzati per fornire agli utenti contenuti pubblicitari rispondenti ai loro interessi secondo il fenomeno della pubblicità comportamentale *online*. Cfr. ROSSI CHAUVENET e STEFANINI, *Internet e* privacy*: il recepimento in Italia della direttiva sulla* cookie law, cit., p. 1808.

[10] ROSSI CHAUVENET e STEFANINI, *op. cit.*, p. 1809.

[11] Che ha modificato la dir. 2002/58 sulla riservatezza nelle comunicazioni elettroniche, c.d. dir. e-privacy (la dir. 2009/136 modificava anche la dir. 2002/22 e la dir. 2006/2004). Tale dir. è attualmente oggetto di un processo di revisione con la Proposta per un Reg. relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche adottata il 10 gennaio 2017.

[12] Il *Data Protection Working Party* era stato costituito in base all'art. 29 della dir. 95/46 Ue ed era composto da un rappresentante delle Autorità di controllo di ciascun Stato membro, da un rappresentante dell'*European Data Protection Supervisor* e da un rappresentante della Commissione europea. HIJMANS, *The European Data Protection Supervisor: The Institutions og the EC Controlled by an Indipendent Authority*, in *Common Market Law Review*, 2006, p. 1313. Al *Working Party Art. 29* è succeduto l'*Editorial Data Protection Board* (EDPB) – costituito in base al Reg. 2016/679 - che è un comitato centralizzato a livello europeo deputato al coordinamento delle azioni delle autorità di sorveglianza attraverso meccanismi vincolanti. Si tratta di un organo indipendente con la propria personalità giuridica il cui ruolo primario risiede nel contributo ad un'applicazione coerente del Regolamento per la protezione dei dati personali in tutta l'Unione europea, nel fare da referente consultivo per la Commissione sul livello di protezione offerto da Stati terzi od organizzazioni internazionali, e nel promuovere la cooperazione tra le autorità nazionali. V. a riguardo IPPOLITI MARTINI, *Comitato europeo per la protezione dei dati*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, dir. da G. Finocchiaro, Bologna, 2017, p. 552 ss.

[13] Cui si può aggiungere anche il Parere 9/2014 sull'applicazione della dir. 2002/58 al *device fingerprinting* come metodo per evitare il ricorso ai *cookie* con il conseguente preventivo consenso dell'interessato, ma ottenere comunque la possibilità di trattare dati dell'interessato. Tale parere avverte che «il *device fingerprinting* ("identificazione dei dispositivi") presenta gravi problemi connessi alla protezione dei dati per le persone. Ad esempio, vari servizi *online* hanno proposto il *device fingerprinting* in alternativa ai *cookie* HTTP allo scopo di fornire dati analitici o di effettuare un *tracking* senza dover richiedere il consenso ai sensi dell'articolo 5, paragrafo 3». «Il messaggio chiave del presente parere è che l'articolo 5, paragrafo 3 della direttiva relativa alla vita privata e alle comunicazioni elettroniche è applicabile al *device fingerprinting*».

[14] V. a riguardo *infra*, note 17, 18.

delle Linee guida sui *cookie* e altri strumenti di tracciamento del giugno 2021, di cui si dirà più avanti al paragrafo 3.

Come si vedrà nel prossimo paragrafo 2 le pratiche di impiego dei *cookie* attualmente in uso da parte degli operatori risultano diffusamente non in linea con la disciplina giuridica del trattamento dei dati personali. Persiste il mancato rispetto di profili di regolazione del trattamento dei dati personali richiesti dalla legge, in primo luogo con riguardo all'acquisizione del consenso dell'interessato al trattamento dei dati quando sia necessario (art. 7, Reg. 2016/679)[15], che deve essere fornito in base ad una informativa trasparente (art. 13, Reg. 2016/679). Per altro verso si vedono impiegate da parte degli operatori pratiche di utilizzo dei *cookie* sempre più aggressive nei confronti degli utenti di internet. Il trattamento dei dati dell'utente in molti casi pare avere il ruolo di una sorta di lasciapassare o di prezzo per l'accesso al sito, e gli operatori si mostrano molto legati a pratiche che consentano loro, eventualmente anche senza il rispetto della disciplina normativa, di attingere ai dati personali di coloro che raggiungono e visitano i loro siti internet[16].

L'utilizzo di *cookie* da parte degli operatori che gestiscono siti internet può peraltro trovarsi in contrasto non soltanto con la disciplina del trattamento dei dati personali ma anche con altre discipline giuridiche, come quelle di tutela del consumatore, per il caso di utenti di internet che siano consumatori, in primo luogo con la disciplina delle pratiche commerciali scorrette e delle clausole vessatorie. Ed anche con la tutela di alcuni diritti fondamentali della persona ulteriori rispetto al diritto sui propri dati personali, ad esempio il diritto all'informazione e il diritto alla libera manifestazione del pensiero. Questi profili saranno esaminati nei prossimi paragrafi 5 e 6.

1. Il quadro normativo del trattamento dei dati personali relativo all'utilizzo dei *cookie* e la trasposizione della disciplina normativa in segni grafici.

Per lungo tempo l'utilizzo dei *cookie* da parte degli operatori in internet non è stato segnalato con il ricorso a segni apparenti sul sito, cosicché gli utenti di internet non avevano di fatto, nel concreto, nemmeno modo di manifestare o negare il loro consenso all'utilizzo di questi ultimi. A meno che non facessero ricorso alla possibilità di bloccare l'operatività dei *cookie* attraverso un'impostazione del *browser* di ricerca da loro utilizzato che li escludesse (anche se si può supporre che questa fosse una possibilità accessibile nei fatti solo agli utenti meno inesperti).

Informazioni grafiche che avvertono l'utente che il sito internet fa ricorso ai *cookie* per trattare i suoi dati personali hanno cominciato ad apparire sui siti internet solo successivamente alla dir. 2009/136 Ue, dopo il parere del 2010 e il documento di lavoro del 2013 dati a livello europeo dal *Working Group Art. 29*, ed in particolare per il nostro Paese successivamente al Provvedimento del Garante della *privacy* del 2014[17] che ha introdotto espresse indicazioni sulla grafica da impiegare per gli avvisi sull'utilizzo dei *cookie* da parte

[15] Presupposti alternativi al trattamento dei dati personali rispetto al consenso sono l'adempimento contrattuale o normativo, l'interesse pubblico, la tutela degli interessi vitali e il legittimo interesse. V. *infra*, nota 55.

[16] L'invito a dare il consenso all'utilizzo dei *cookie* è a volte accompagnato da informazioni del tipo che la raccolta dei dati svolge la funzione di offrire all'utente una migliore esperienza sul sito visitato.
Già nel 2010 il *Working Party Art. 29* nel suo parere 2/2010, del 22 giugno 2010, WP 171, p. 4, rilevava «il crescente ricorso alla pubblicità comportamentale, che si basa sull'impiego di marcatori ("*cookie*") e di altri dispositivi analoghi, e il suo alto livello di intrusione sulla vita privata».

[17] Provvedimento del Garante della *privacy*, 8 maggio 2014, "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei *cookie*". Seguito dalle FAQ "Informativa e consenso per l'uso dei *cookie*" del 3 novembre 2014 e dai "Chiarimenti in merito all'attuazione della normativa in materia di *cookie*" del 5 giugno 2015.

degli operatori su internet[18].

A chiarire che l'utilizzazione dei *cookie* è sottoposta alla disciplina del trattamento dei dati personali e al preventivo consenso al trattamento dei dati – all'epoca contenuta nella dir. 95/46 – aveva contribuito la dir. 2009/136 del 25 novembre 2009, che aveva all'epoca rivisto sotto tale profilo la dir. 2002/58, nota come *e-Privacy Directive*[19], introducendo al suo art. 5.3 la previsione secondo la quale la memorizzazione di informazioni o l'accesso ad informazioni già memorizzate sul supporto di un utente è consentito soltanto a condizione che questi abbia dato il suo consenso. Sull'utilizzo dei *cookie* è di interesse anche il considerando 66 della dir. 2009/136 che fa riferimento alla circostanza che «il consenso dell'utente al trattamento può essere espresso mediante l'uso delle opportune impostazioni di un motore di ricerca o di un'altra applicazione, qualora ciò si riveli tecnicamente fattibile ed efficace, conformemente alle pertinenti disposizioni della dir. 95/46». Considerando che tuttavia si è ritenuto non possa di per sé far ritenere che le impostazioni del *browser* siano una sufficiente espressione del consenso al trattamento dei dati a mezzo dei *cookie*[20]. Nel suo parere 1/2009 del 10 febbraio 2009 il *Working Group Art. 29* (WG) aveva rilevato l'inadeguatezza dell'approccio della dir. 2002/58 - che la dir. 2009/163 aveva poi modificato - a garantire il rispetto del diritto dell'utente sui propri dati personali come previsto dalla dir. 95/46 all'art. 2 lett. *h*. Il WG si era espresso nel senso che «le impostazioni predefinite di molti programmi di navigazione non consentono all'utente di essere informato circa i tentativi di memorizzazione o di accesso alla sua apparecchiatura terminale. Le impostazioni predefinite dei programmi di navigazione (…) non possono (…) essere un mezzo per l'utente di manifestare la propria volontà libera, specifica e informata, come richiesto dall'art. 2, lettera *h*), della direttiva sulla tutela dei dati. Per quanto riguarda i *cookie* il gruppo è del parere che

---

[18] Nel Provvedimento del Garante per la protezione dei dati personali dell'8 maggio 2014 cit. *supra*, nota prec., viene indicato come i *cookie* devono essere segnalati all'utenza da parte dei siti internet in aggiunta alla regolazione generale di cui all'art. 122 cod. privacy (introdotta in attuazione della dir. 2009/136 dal d.lgs. n. 69 del 2012).

Per la manifestazione del consenso al trattamento dei dati personali attraverso *cookie*, non necessario per i c.d. *cookie* tecnici (ossia, si deve intendere, quelli necessari, ma v. ora il Provvedimento n. 231 del 2021 su cui *infra*, par. 3), il Garante ha indicato che dev'essere evidente sul sito, non appena lo si raggiunga, un'informativa sintetica (secondo la previsione dell'art. 122, 1° co. che rinvia all'art. 13, 3° co. dell'allora cod. privacy) cui si deve aggiungere un'informativa estesa di secondo livello che deve contenere tutti gli elementi previsti dall'art. 13 cod. privacy, illustrando nel dettaglio le finalità del trattamento dei dati per quegli utenti che decidano di voler accedere ad informazioni di livello più approfondito sulla tutela dei dati. All'interno di tale informativa dev'essere inserito anche il *link* aggiornato alle informative e ai moduli di consenso delle terze parti con le quali il titolare ha stipulato accordi per l'installazione di *cookie* tramite il proprio sito. Qualora il titolare abbia contatti indiretti con le terze parti dovrà inserire i *link* ai siti dei soggetti che fanno da intermediari tra lui e le stesse terzi parti. Tale tecnica di informativa dell'utenza e di acquisizione del consenso trova ragione nel contemperamento delle ragioni di tutela dei dati dell'utente con le attività di significato economico che sono sorte con la navigazione *online*.

[19] POLINI, Privacy *e protezione dei dati personali nell'ordinamento europeo e italiano*, in *Manuale di diritto alla protezione dei dati personali*, a cura di Maglio, Polini, Tilli, Rimini, Maggioli, 2017, p. 45, «la direttiva (…) 95/46/CE ha fissato i principi generali della normativa in materia di dati personali per consentire la libera circolazione dei dati personali nel territorio europeo mentre le direttive (…) 2002/58/CE e 2009/136/UE relative al "trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche" hanno introdotto alcune precisazioni specifiche rispetto alla direttiva 95/46 che riguardano la raccolta di dati personali effettuata *on line* e in particolare l'utilizzo dei *cookie*».

[20] Cfr. ROSSI CHAUVENET e STEFANINI, *Internet e* privacy*: il recepimento in Italia della direttiva sulla* cookie law, cit., pp. 1813-1815. Che richiamano sul punto MANTELERO, *Observatory on ITC Law: new rules and technical solutions concerning cookies and other device to profile internet users*, in *Contr. Impr./Eur.*, 2011, p. 811, che esclude appunto che il considerando 66 della dir. 2009/136 costituisca una base legislativa sufficientemente forte per affermare che le impostazioni dei *browser* degli utenti siano una valida forma per la manifestazione del consenso a ricevere *cookie* da parte degli interessati.

chi si avvale di questi dispositivi debba informarne l'utente nella dichiarazione sulla riservatezza e non far affidamento alle impostazioni (predefinite) dei programmi di navigazione. Peraltro la formulazione prescelta non si limita ai *cookie* ma include qualsiasi tecnologia atta ad individuare il comportamento dell'utente del programma di navigazione».

La dir. 2009/136 si era inserita nel quadro di riforma europeo delle reti e dei servizi di comunicazione elettronica segnando nella regolazione dei *cookie* l'importante passaggio da un approccio "*opt-out*", in base al quale doveva essere garantita all'utente la possibilità di rifiutare l'installazione dei *cookie*, ad un approccio "*opt-in*" che impone invece di ottenere il consenso dell'utente per qualsiasi utilizzo non strettamente connesso con il servizio reso[21]. Ha infatti espressamente imposto in capo ai fornitori di servizi internet, come si è sopra visto, l'obbligo per i titolari (o i responsabili) del trattamento dei dati personali di ottenere il previo consenso informato dell'utente per l'archiviazione di informazioni o l'accesso delle informazioni già archiviate nel suo terminale[22].

Nel 2010 il *Working Group Art. 29* aveva successivamente fissato l'attenzione sull'utilizzazione dei *cookie* come pratica di pubblicità comportamentale che, nonostante i benefici sotto il profilo commerciale - affermava il WG -, non poteva essere impiegata a spese della protezione del diritto individuale al rispetto della vita privata e alla protezione dei dati personali dell'utente di internet[23]. Il parere aveva rilevato che nell'utilizzo dei *cookie* diretti al monitoraggio del comportamento *online* degli utenti allo scopo di fornire pubblicità mirata – che può avere una portata di rilievo sotto il profilo temporale soltanto nell'immediato, oppure prolungata - fosse importante il rispetto della dir. 95/46 quale discipina del trattamento dei dati personali. Aveva affermato inoltre che attenzione massima dovesse essere dedicata al profilo della trasparenza, di particolare rilievo per assicurare che il consenso venisse prestato efficacemente.

Il *Working Document* 2/2013 del *Working Group Art. 29* sul consenso all'uso dei *cookie* si era soffermato sulle modalità pratiche cui far ricorso da parte degli operatori per ottenere il consenso al loro utilizzo in linea con la disciplina del trattamento dei dati personali data a livello europeo (che nel 2013 era ancora la dir. 95/46). Ed in particolare sui requisiti dell'informativa specifica, sulla necessità di acquisire il consenso prima dell'inizio del trattamento, sulla scelta attiva da parte dell'interessato, sulla libertà del consenso. Requisiti questi che, come si vedrà più avanti, al par. 4, sono stati riaffermati anche in tempi successivi e recenti da decisioni della Corte di giustizia Ue rispetto alle pratiche utilizzate dagli operatori. Importante è anche il parere 3/2013 del *Working Group Art. 29* che si è soffermato sulla limitazione dello scopo per il trattamento dei dati personali, requisito che contribuisce alla trasparenza, alla certezza legale e alla prevedibilità, ed è diretto a proteggere l'interessato fissando i limiti entro i quali i responsabili possono trattare i dati. Il concetto di limitazione dello scopo è costituito da due concetti principali: i dati personali devono essere raccolti per scopi specifici, espliciti e legittimi (specificazione di scopo) e non possono essere trattati in modo incompatibile con tali scopi (uso compatibile).

La regolazione del consenso al trattamento dei dati personali, preceduto dall'informativa,

---

[21] ROSSI CHAUVENET e STEFANINI, *op. cit.*, p. 1814.

[22] Ed inoltre per i titolari (o i responsabili) del trattamento di attuare le adeguate misure di protezione contro possibili perdite o diffusioni incontrollate dei dati e, per il caso di violazioni dei dati personali, di informare tempestivamente le autorità di vigilanza e gli utenti, oltre all'obbligo di adottare misure appropriate per garantire che le comunicazioni indesiderate a scopo di *marketing* siano permesse solo a fronte del consenso degli utenti interessati.

[23] *Article 29 Data Protection Working Party*, WP 171, *Opinion 2/2010 on online behavioural advertising*, 22 giugno 2010.

è ora contenuta nel Reg. 2016/679[24], e relativamente a tale disciplina e alle sue applicazioni rispetto ai *cookie* sono intervenuti più pareri delle Autorità garanti, compreso lo *European Data Protection Board* (che è succeduto nelle funzioni del *Working Group Art. 29*), e pronunce giurisprudenziali che ne hanno chiarito la portata.

Il Reg. 2016/679 definisce il consenso al trattamento dei dati personali ai suoi artt. 4.11, 6.1 lett. *a*, 7 e nel considerando 32. In linea con l'art. 4 il consenso è una manifestazione di volontà libera, specifica, informata (l'informativa che deve precedere il consenso è regolata dall'art. 13) ed inequivocabile dell'interessato. L'art. 6 del Reg. 2016/679 prevede che il consenso al trattamento debba essere dato per una o più finalità specifiche. Il considerando 32 afferma che il consenso deve essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata ed inequivocabile di accettare il trattamento dei dati personali che lo riguardano, e che se il consenso abbia più finalità dovrebbe essere prestato per ognuna di queste. Più in generale il considerando 7 afferma che è opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano[25]. Tali previsioni normative sono di fondamentale importanza per la regolazione dell'utilizzo dei *cookie* e per indicare i requisiti che devono accompagnare il consenso al trattamento dei dati personali operato attraverso i *cookie*.

Il trattamento dei dati personali attraverso l'impiego di *cookie* va quindi evidenziato all'utente di internet con indicazioni grafiche dirette ad acquisire il suo consenso attraverso modalità che siano allo stesso tempo trasparenti per l'utente (art. 5.1 lett. *a* e art. 12 Reg. 2016/679 su informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato, e anche art. 2, lett. *e* cod. consumo sul diritto dei consumatori alla trasparenza nei rapporti contrattuali[26]) e sintetiche, in modo tale da poter essere visualizzate al raggiungimento di un determinato sito internet. Tali indicazioni grafiche consistono in *banner* che appaiono sulla pagina del sito internet raggiunta dall'utente e contengono un'informativa di primo livello accompagnata da una informativa più dettagliata, detta di secondo livello, di solito raggiungibile attraverso un *link*[27], che completa gli elementi che la legge (ora la

---

[24] «In capo al titolare del trattamento sono posti obblighi di trasparenza più stringenti rispetto alla precedente normativa. I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità», POLINI, *op. cit.*, p. 47.
In via generale il Reg. 2016/679 introduce per il consenso come presupposto per il trattamento dei dati personali dei requisiti e delle specificazioni di maggiore precisione rispetto alla normativa precedente. La definizione di consenso è più dettagliata attraverso la previsione dell'art. 7 e di diversi considerando che ne descrivono in maniera pratica ed analitica le condizioni di validità e le regole relative all'onere probatorio, mentre l'art. 8 viene specificamente dedicato al consenso dei minori ai servizi della società dell'informazione. La dir. 95/46 aveva introdotto il consenso tra i presupposti per il trattamento dei dati personali, e il consenso aveva poi trovato una menzione nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea. Si riferisce che successivamente si era via via assistito ad uno snaturamento del consenso attraverso una raccolta di dati personali sempre più intensa, cui andava di pari passo la diffusione di un modo di intendere il consenso, una volta che esso si fosse ottenuto, con qualsiasi modalità, come presupposto giustificativo in maniera generalizzata di qualsiasi trattamento dei dati personali. A tale snaturamento del consenso avevano cercato di far fronte le autorità di protezione dei dati precisando i requisiti del consenso richiesti dalla direttiva e dalle legislazioni nazionali. Tali interventi hanno appunto poi trovato una collocazione nel successivo Reg. 2016/679. M.C. MENEGHETTI, *Consenso* bis*: la Corte di Giustizia torna sui requisiti di un valido consenso* privacy, in *Medialaws.it*, n. 1/2021, 11 aprile 2021.

[25] PIZZETTI, *Il futuro dell'Europa si regge sui dati*, consultato *online*, rileva che tale considerando si connette all'art. 20 del Reg. 2016/679 sulla portabilità dei dati ma e che il controllo della persona sui propri dati è un'espressione che può anche essere interpretata in modo estensivo con riferimento ai dati prodotti da una persona anche solo accedendo a servizi *online*.

[26] Come si vedrà più avanti nel testo anche il *Working Group Art. 29* aveva posto l'accento sull'importanza del rispetto della trasparenza.

[27] Questo per non aggravare la chiarezza sotto il profilo grafico e dello spazio occupato sul sito dalle informazioni che devono essere date per acquisire un consenso il più possibile consapevole da parte dell'utente.

previsione dell'art. 13 Reg. 2016/679[28]) richiede per l'informativa che deve precedere il consenso dell'interessato[29]. Questi elementi grafici erano già stati indicati esplicitamente dal citato Provvedimento del Garante della *privacy* del 2014. Si abbia presente che la versione dell'art. 122 del cod. privacy, successiva al 2018 (quando si è avuto l'adattamento della disciplina italiana al Reg. 2016/679) e attualmente in vigore, ha indicato il ricorso ad una informativa abbreviata[30]. Nell'Allegato 1 alla Consultazione sulle "Linee guida sull'utilizzo dei *cookie* e di altri strumenti di tracciamento" del novembre 2020 si è indicato che sempre all'interno dell'area dedicata al consenso all'uso dei *cookie* dovrebbero trovare collocazione due ulteriori comandi idonei a garantire il diritto di ripensamento e di revoca del consenso agli utenti che, avendo già effettuato una specifica scelta al momento del primo accesso al sito *web* intendano successivamente optare per una scelta diversa[31]. Le Linee guida del Garante del giugno 2021 prevedono che nel *banner* utilizzato ai fini dell'acquisizione del consenso sia inserito un *link* ad un'area nella quale poter scegliere, tra l'altro, di revocare il consenso già espresso (Allegato I alle Linee guida, sezione Informativa e consenso, lett. *f*).

Oltre al principio di trasparenza, già citato sopra, altro principio di rilievo generale nel Regolamento, e applicabile perciò anche nelle pratiche utilizzo dei *cookie*, è il principio di minimizzazione nel trattamento dei dati.

Quanto alle novità più recenti, il testo della Proposta del nuovo Regolamento UE sulla *e-privacy* (del 2017) come approvato nel febbraio 2021 dal Consiglio dell'Unione Europea (e ora soggetto all'approvazione del Parlamento UE) interviene sulla regolazione dei *cookie* prevedendo, al fine di ovviare a quella che viene definita come *cookie fatigue*, l'indicazione (ma non l'obbligo) per gli operatori di prevedere delle impostazioni di *default* che consentano agli utenti finali di gestire il consenso ai *cookie* in maniera agevole e trasparente, facendo delle scelte in merito all'archiviazione e all'accesso ai dati memorizzati, attraverso l'impostazione e la modifica di *whitelist* per categorie di *cookie* accettate o meno[32]. Questo prospettato intervento pare si presti a contrassegnare di novità le pratiche relative all'impiego dei *cookie*, assieme al progressivo allontanamento dall'impiego dei *cookie* di terze parti preannunciato dai motori di ricerca (su cui ci si soffermerà nel par. delle conclusioni).

2. Le pratiche adottate dagli operatori nell'utilizzazione dei *cookie.*

Se certo non manca il ricorso a pratiche che si attengono alle prescrizioni normative con l'acquisizione del consenso specifico, attivo ed inequivoco dell'interessato all'impiego di *cookie* (con l'indicazione di quali dati personali saranno trattati e per quali scopi) preceduto dall'informativa[33], molti operatori ricorrono all'utilizzo di *cookie* attraverso pratiche che con

---

[28] Il consenso al trattamento dei dati personali dev'essere dato in base appunto ad un'informativa specifica comprensiva dell'indicazione degli scopi per i quali i dati sono trattati, della base giuridica del trattamento, dei destinatari o le eventuali categorie dei destinatari cui i dati sono destinati, del periodo di conservazione dei dati, tra le indicazioni principali (art. 13 Reg. 2016/679).

[29] Ed in base alla quale egli esprime il suo consenso al trattamento dei dati personali.

[30] La norma prevede ora che – ad eccezione dei c.d. *cookie* tecnici - «l'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate».

[31] V. "Linee guida sull'utilizzo dei *cookie* e di altri strumenti di tracciamento" del nostro Garante della *privacy* del novembre 2020, p. 10.

[32] Viene da osservare che tali possibili impostazioni di *default* dovranno comunque essere sostanzialmente differenti dai *browser setting* impiegati nel passato, esclusi dall'ammissibilità quanto all'impiego per la manifestazione del consenso ai *cookie* anche nella più recente versione delle *Guidelines* del CNIL francese dell'ottobre 2020.

[33] Altro punto in senso logico è poi se l'osservanza delle prescrizioni normative sia nella sostanza sufficientemente protettiva dell'utente/interessato.

esse non si allineano. E, anzi, come si diceva sopra, negli ultimi tempi si riscontrano comportamenti degli operatori diretti al trattamento e alla raccolta dei dati personali attraverso i *cookie* sempre più aggressivi nei confronti degli utenti[34].

Alcuni esempi delle pratiche di diffuso impiego da parte degli operatori si possono ricondurre alle seguenti tipologie:

- pratiche che impiegano un *banner* che fa avviso dell'utilizzo di *cookie*, ed eventualmente contiene un *link* alle condizioni di trattamento dei dati, ma non richiede all'utente un consenso espresso (attivo) rispetto all'uso dei *cookie*;

QUESTO SITO USA I COOKIE!
Lo facciamo per mostrarti i nostri prodotti e servizi e per poterti offrire la migliore esperienza possibile. Se sei d'accordo con questo, prosegui pure e buona navigazione!
Scopri di più OK

- pratiche che richiedono all'interessato un consenso generale/generico relativo all'uso di più *cookie* in maniera congiunta come quelli necessari, funzionali, analitici, previa informativa cui si accede tramite *link*;

Questo sito utilizza i propri cookie per migliorare la tua esperienza di navigazione e terze parti per inviarti messaggi promozionali in linea con le tue preferenze. Per ulteriori informazioni e per modificare le impostazioni dei cookie, fare clic su "ulteriori informazioni".

Se si fa clic sul pulsante "OK" o se si continua a navigare, si accetta l'uso dei cookie - ulteriori informazioni ok

- pratiche che richiedono all'interessato, previa informativa, il consenso all'utilizzo di determinati *cookie* attraverso caselle già pre-spuntate, che l'utente può deselezionare se intende negare il consenso alla raccolta, o che a volte non possono nemmeno essere deselezionate;
- pratiche che richiedono il consenso all'interessato con la formulazione dell'informativa con cui i dati personali sono raccolti e per quali scopi in modo poco chiaro, quanto al testo e/o alla grafica impiegata;
- impiego di avvertenze preliminari al trattamento dei dati mediante *cookie* dal significato ingannevole, quali ad esempio espressioni secondo le quali "l'operatore ha massima cura dei dati personali dell'utente" e per questo procede al trattamento dei dati dell'utente, che vengono raccolti per vari scopi, usualmente anche di profilazione;

La vostra privacy è per noi molto importante
Noi e i nostri partner conserviamo e/o accediamo alle informazioni su un dispositivo, come gli ID univoci nei cookie per il trattamento dei dati personali. È possibile accettare o gestire le vostre scelte cliccando qui sotto, compreso il vostro diritto di opporvi in caso di utilizzo di interessi legittimi, o in qualsiasi momento nella pagina della privacy policy. Queste scelte verranno segnalate ai nostri partner e non influenzeranno i dati di navigazione.**Cookie policy**
Noi e i nostri partner trattiamo i dati per fornire:
Utilizzare dati di geolocalizzazione precisi. Scansione attiva delle caratteristiche del dispositivo ai fini dell'identificazione. Archiviare e/o accedere a informazioni su un dispositivo. Annunci e contenuti

[34] Anche ad esempio attraverso il trattamento dei dati personali tramite *application* (*App*), in *Il Sole24 ore*, 14 dicembre 2020.

- ricorso a *banner* per la richiesta del consenso al trattamento dei dati personali che occupano fisicamente buona parte della pagina *web*, provocando il fastidio dell'utente che così tende a dare il consenso prima possibile per superare la sensazione di fastidio, e sollecitando l'impressione dell'utente di non poter procedere nella navigazione se non accordi il suo consenso all'utilizzazione dei *cookie*;

- pratiche di "falso consenso" come saranno descritte più avanti, al paragrafo 4;

- ricorso da parte degli operatori al proprio legittimo interesse al trattamento dei dati personali impiegando caselle preselezionate che devono essere deselezionate dall'utente/interessato (o a volte caselle da selezionare da parte dell'utente) per negare all'operatore la raccolta dei dati in base al proprio legittimo interesse (o per accordare il consenso alla raccolta in base al legittimo interesse) (il legittimo interesse trova base nel considerando 47 del Reg. 2016/679 e nell'art. 6.1 lett. *f*).

Altra pratica in uso da parte dagli operatori di internet su cui va portata l'attenzione è quella del ricorso ai c.d. *cookie wall*. Si devono infatti distinguere i casi nei quali, in mancanza di consenso alla raccolta dei dati per alcune finalità, la navigazione è comunque consentita, da quelli in cui viene impedito l'accesso ai contenuti del sito, o ad alcuni contenuti del sito. Tale ultima pratica che impedisce l'accesso al sito nel caso del mancato consenso al trattamento dei suoi dati personali da parte dell'utente viene appunto definita con l'espressione di *cookie wall*, e la sua legittimità alla luce del GDPR è discussa[35].

Altre pratiche impiegate dagli operatori che gestiscono siti internet osservano invece effettivamente l'obbligo di richiedere il consenso specifico, attivo ed univoco dell'interessato per ogni singola tipologia di *cookie*. Il consenso dev'essere come si è visto sopra preceduto dall'informativa, sintetica e poi più dettagliata, cui si accede in via separata[36], in linea con le previsioni generali che regolano normativamente il trattamento dei dati personali e con le indicazioni che ha dato il Garante nel Provvedimento del 2014 che si è sopra citato. Non si può comunque non osservare come l'utilizzo dei *cookie* da parte degli operatori, anche nel caso in cui rispetti le prescrizioni previste dalla legge, metta comunque nel concreto gli utenti regolarmente e mediamente in una situazione di soggezione, dato che si tratta di pratiche che

[35] Le *Guidelines* adottate dal CNIL nel luglio 2019 reputavano tale pratica contraria al GDPR riprendendo l'opinione dello *European Data Protection Board* (EDPB). Successivamente una sentenza del Consiglio di Stato francese del giugno 2020 ha contestato la validità dell'opinione espressa in merito dal CNIL in ragione del fatto che un divieto di fare ricorso ai *cookie wall* non si potrebbe far derivare dalla previsione generale del GDPR secondo la quale il consenso deve essere dato liberamente né dal – non vincolante – parere dello EDPB in quest'ultimo senso. La nuova versione delle *Guidelines* sui *cookie* del CNIL è stata pubblicata il 1° ottobre 2020 ed è entrata in vigore ad aprile 2021. Quanto ai *cookie wall* le Linee guida prevedono che la legittimità del ricorso ai *cookie wall* sarà valutata caso per caso; ad ogni modo gli operatori devono chiaramente informare gli utenti sulle conseguenze dell'accettazione o del rifiuto dei *cookie*, ovvero gli utenti devono essere informati della impossibilità di avere accesso al servizio qualora rifiutino i *cookie*. Si esprime in merito ai *cookie wall* anche l'Allegato 1 alla Consultazione sulle "Linee guida sull'utilizzo dei *cookie* e di altri strumenti di tracciamento" del nostro Garante della *privacy* del novembre 2020, p. 7, cit. *supra*, nota 6, affermando che tale meccanismo non consente di qualificare il consenso quale conforme al Regolamento e in particolare al suo art. 4.11, e quindi è da ritenersi illecito salva l'ipotesi, da verificare caso per caso, in cui il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di *cookie*. Questa prospettiva è stata confermata dalle Linee guida adottate dal Garante nel giugno 2021 a conclusione della Consultazione, come si vedrà *infra*, nel testo, al par. 3.

[36] Pena, attraverso l'impiego di una informativa di primo livello molto dettagliata, il risultato non di informare meglio l'interessato, ma di essere in definitiva poco trasparenti, e confondere l'utente con un eccesso di informazioni.

difficilmente sono pienamente comprese se non da utenti davvero esperti[37].

Quanto all'utilizzazione dei *cookie* su internet è probabilmente calzante a descrivere la posizione dell'utente l'espressione di "vulnerabilità strutturale dell'individuo", che è stata impiegata all'osservazione delle pratiche di trattamento dei dati personali nella società contemporanea[38]. Tale posizione di soggezione diventa naturalmente ancor più grave nel caso di persone che sono di regola ancor più vulnerabili, come ad esempio i minori di età (considerando 38 e 58 Reg. 2016/679).

Per quanto concerne l'utente di internet che sia consumatore, ne mette in rilievo la posizione di vulnerabilità il rapporto del marzo del 2021 del *Bureau Européen des Unions des Consommaterurs* (BEUC) dal titolo "EU Consumer Protection 2.0 – Structural asymmetries in digital consumer market" che evidenzia come sia necessario introdurre modifiche al diritto europeo dei consumatori per tutelare i consumatori digitali.

Forse, eventualmente, solo l'adozione di una grafica molto chiara, semplice, ed imposta in via uniforme potrebbe temperare la situazione di soggezione dell'individuo/interessato. A tal proposito potrebbe essere di grande utilità lo sviluppo e la diffusione del ricorso alle tecniche di *legal design* sulle quali si sta in effetti lavorando e che promettono sviluppi per il prossimo futuro[39]. Al proposito anche il Garante per la protezione dei dati personali nell'Allegato 1 alla Consultazione sulle "Linee guida sull'utilizzo dei *cookie* e di altri strumenti di tracciamento" del novembre 2020 sottolinea l'importanza di una «riflessione sulla necessità dell'adozione di una codifica standardizzata relativa alla tipologia dei comandi, dei colori e delle funzioni da implementare all'interno dei siti *web* per conseguire la più ampia uniformità, a tutto vantaggio della trasparenza, della chiarezza e dunque anche della migliore conformità alle regole»[40].

In linea più generale, a proposito dell'utilizzo dei *cookie* potrebbero rivelarsi calzanti i dibattiti sul requisito fondante della disciplina europea del trattamento dei dati personali, ossia sul consenso dell'interessato quale presupposto per il trattamento dei dati personali. In effetti il presupposto del consenso, in astratto certo imprescindibile e protettivo della volontà dell'interessato rispetto al trattamento dei suoi dati personali, spesso può non sostanziarsi in un elemento efficace a proteggere la posizione della persona interessata, considerato anche che nei fatti potrebbe non sempre trattarsi di un consenso davvero consapevole[41]. Non si

---

37 Si potrebbe prospettare un parallelismo con la regolazione dei rapporti sui mercati finanziari rispetto alla quale pure la regolazione del consenso sulla base delle informazioni fornite è suscettibile di mettere in difficoltà l'investitore. Rileva PERRONE, *Servizi d'investimento e tutela dell'investitore*, in *Banca, borsa, tit. credito*, 2019, p. 3 s., che a seguito degli scandali di inizio secolo e della crisi finanziaria globale è emersa la consapevolezza dell'«insufficienza di una disciplina di mera trasparenza, che può "persino legittimare pratiche perniciose" a detrimento di chi pur sarebbe diretta a proteggere».

38 Espressione utilizzata ed individuata dal prof. Pasquale Stanzione Presidente dell'Autorità garante per il trattamento dei dati personali nella sua relazione al Workshop Protech del 16 ottobre 2020. Si veda STANZIONE, *Data Protection and Vulnerability*, in *EJPLT*, 2, 2020, p. 9 ss.

39 Negli ultimi anni c'è stato uno sviluppo sensibile dell'attenzione e dello studio del *legal design*. V. AULINO, *Consenso al trattamento dei dati e carenza di consapevolezza: il* legal design *come rimedio* ex ante, in *Dir. inf. inform.*, 2020, p. 303-312; AULINO, *Legal design and A.I. in support of legislative drafting during crisis*, in *EJPLT*, 1, 2020, pp. 173-176; AULINO, *La comprensione effettiva dei testi giuridici da parte del consumatore. Scienze comportamentali e* legal design, in *Manuale di Diritto e tutela del consumatore*, in *Strumenti per la didattica di diritto civile*, a cura di L. Gatt, in corso di pubblicazione.

40 V. "Linee guida sull'utilizzo dei *cookie* e di altri strumenti di tracciamento", cit., p. 10.

41 GATT, MONTANARI, CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale*, in *Pol. dir.*, 2017, pp. 350-351, dove si mettono in rilievo «i limiti del *consenso* preventivo sia perché reso inconsapevolmente sia perché - anche quando è reso consapevolmente – non si traduce in un effettivo impedimento alla dannosità del trattamento per la persona dell'utente. Al contrario, la prestazione del consenso potrebbe avere un effetto distorsivo perché esso viene prestato senza che l'utente abbia cognizione degli strumenti di tutela *ex post* ed anzi sulla base della convinzione che la sola concessione del consenso elimini *a*

deve sottostimare la circostanza che gli utenti di internet, a certe condizioni e di fronte all'offerta di servizi apparentemente gratuiti, sono comunque portati a cedere propri dati personali. Per cui, rispetto a comportamenti degli operatori ampiamente diffusi, tendenzialmente prevaricatori della posizione degli utenti, a volte anche in maniera subdola, paiono poter essere efficaci soltanto divieti e/o prescrizioni di risarcimento dei danni[42].

3. Interpretazioni recenti della disciplina del trattamento dei dati personali in relazione all'uso dei *cookie*, azioni e rimedi per il mancato rispetto dei diritti dell'interessato.

I principi e i caratteri del consenso al trattamento dei dati personali - quindi anche quello relativo all'uso dei *cookie* – sono stati chiariti dalle *Guidelines* n. 5/2020 dell'*European Data Protection Board* (EDBP)[43] del 4 maggio 2020 sul consenso nel Reg. 2016/679[44] che hanno

priori la possibilità stessa di una lesione». «La sperimentazione condotta e le analisi giuridico-comportamentali dei dati raccolti evidenziano (…) l'inefficienza di una tutela *ex ante* che si sostanzi in un divieto di trattamento dei dati (sicuramente di quelli non-sensibili) e fanno propendere per l'ideazione di uno speciale statuto di circolazione (regolamentazione del trattamento) quantomeno per dati non sensibili, in un'ottica finale di elaborazione di un rimedio privatistico risarcitorio/restitutorio in funzione di deterrenza ai trattamenti dannosi per l'utente (vale a dire, di un'effettiva ed efficiente tutela *ex post*)». Gli studi condotti (e si rinvia al proposito a BEN-SHAHAR e CHILTON, *Simplification of Privacy Disclosures: An Experimental Test*, in *University of Chicago Coase-Sandor Institute for Law & Economics, Research Paper* n. 737, 2016) «rivelano che, in modo più o meno consapevole, l'informativa non è letta e pertanto il consenso prestato non è consapevolmente fornito». «Il riscontrato atteggiamento verso la lettura o consultazione dell'informativa *privacy* nonché il più generale collegamento con le singole attività cui il trattamento afferisce può indurre a considerare come il miglioramento delle modalità di redazione e della chiarezza dell'informativa, che pure rappresenta un costante obiettivo delle politiche comunitarie e nazionali anche attraverso le autorità di controllo, ragionevolmente non sia destinata a produrre significativi cambiamenti nel grado di consapevolezza degli utenti» (pp. 348-349).

[42] MANTELERO, *Regulating big data. The Guidelines of the Council of Europe in the Context of the European data protection framework*, in *Computer Law & Security Review*, 2017, pp. 584-602, mette in rilievo che nel contesto completamente nuovo venutosi a creare nell'ultimo decennio «data are abundant, in some cases excessive and redundant, information is constantly reused, analytics are able to extract predictive information from data sets and algorithms are increasingly becoming part of decision making processes. All of these changes undermine the foundational idea that data subjects' self-determination is expressed through their meaningful consent to data processing, because data subjects are not able to cope with the complexity, and often obscurity, of today's information uses. The big data paradigm also undermines the very notion of "specified purpose", in terms of the scope of data processing which should be known and defined at the moment of data collection». «The data subject's consent, when required, becomes an easy way to legitimise any sort of data processing and further re-use information». L'impostazione del Reg. 2016/679 non si distacca da quella della dir. 95/46, risalente agli anni '90, anche in ragione del successo a livello internazionale incontrato da questo modello ma, mette in evidenza l'a., «the technology scenario of the '90 is far from removed from our daily experience. At that time, data were still collected and processed for a limited range of purposes (e.g. loyalty programs) and the level of complexity of data analysis was still understandable by users. Today, powerful analytics make it possible to extract unpredicted inferences from large amounts of data, which are extensively collected for generic purposes and processed in a manner that is often obscure and usually unintelligible. This necessarily raises the question of whether the data protection paradigma as defined in Directive 95/46/EC – and confirmed in Regulation (EU) 2016/679 – is still adequate to address the challenges of this new scenario». Di fronte all'affermazione dei c.d. *big data* per le tecnologie di attuale diffusione come la *Internet of Things* e l'intelligenza artificiale è essenziale la disponibilità di grandi quantità di dati personali e per tali raccolte la strada più praticabile è quella del trattamento di dati in modo anonimizzato, e in tali casi il consenso non costituisce da premessa al trattamento. Più che le diffuse tecniche di anonimizzazione si stanno diffondendo, allo scopo di scindere i dati personali dagli elementi di realtà che li legano alla persona fisica da cui provengono, tecniche di *machine learning* per la realizzazione di dati sintetici.

[43] Questo organismo è succeduto al *Working Group Art. 29* come si è visto *supra*, a nota 12.

[44] Queste Linee Guida rivedono una delle prime *Guidelines* date in precedenza dal *WP Art. 29* nell'aprile 2018 per porre rimedio alle divergenze sull'interpretazione di cosa costituisca consenso con speciale riguardo ai *cookie* e alle altre tecnologie di tracciamento.

approfondito l'interpretazione delle nozioni di consenso informato, consenso libero, consenso attivo (e manifestato in maniera inequivocabile), consenso specifico e per il singolo scopo, trasparenza. Lo *European Data Protection Board* (EDPB) ha specificato tra l'altro che non sono consentite caselle preselezionate nei *banner* dedicati alla manifestazione del consenso all'utilizzo dei *cookie*; che la continuazione della navigazione su un sito internet non può equivalere alla manifestazione di un consenso attivo ed espresso, quindi non può significare consenso al trattamento dei dati personali; che il consenso all'utilizzo dei *cookie* nel caso di impiego *cookie wall* non è un consenso valido in quanto si fa dipendere l'accesso al sito dall'accettazione dei *cookie* cosicché il consenso non si può reputare dato liberamente[45]. Le Linee Guida prevedono anche che se un operatore ha come pubblico di riferimento un pubblico di minori deve adeguare le pratiche al suo pubblico.

Recentemente sono state pubblicate sul tema le *Guidelines* adottate dall'Autorità garante francese (CNIL) nel luglio 2019, poi riviste in una nuova versione pubblicata il 1° ottobre 2020 che è entrata in vigore ad aprile 2021, e le *Guidance Note: Cookies and other tracking technologies* dell'aprile 2020 della *Data Protection Commission* irlandese che costituiscono un punto di riferimento per la ricostruzione in termini concreti della disciplina da applicare alle pratiche di impiego dei *cookie*. Nel novembre 2020 il nostro Garante per la protezione dei dati personali ha aperto una Consultazione sul documento "Linee guida sull'utilizzo dei *cookie* e di altri strumenti di tracciamento" per valutare le pratiche in uso relative ai *cookie* e a tali altri strumenti[46]. La consultazione si è chiusa con l'adozione delle "Linee guida sui *cookie* e altri strumenti di tracciamento" del giugno 2021 (Provvedimento n. 231 del 10 giugno 2021) che fa da aggiornamento alle precedenti Linee guida del 2014. Tali Linee guida recentemente pubblicate precisano che nel rispetto del Regolamento 2016/679 UE l'informativa agli utenti dovrà specificare anche gli eventuali altri soggetti destinatari dei dati personali e i tempi di conservazione delle informazioni. È confermato che solo per i *cookie* tecnici è necessaria la sola informativa – senza l'espressione di un esplicito consenso – e si raccomanda che i *cookie analytics*, usati per valutare l'efficacia di un servizio, siano utilizzati solo a scopi statistici (e in tal caso sono trattati come *cookie* tecnici). Il Garante afferma che dovrà essere offerta agli utenti la possibilità di proseguire la navigazione anche senza essere in alcun modo tracciati. Il *cookie wall* deve ritenersi illegittimo salva l'ipotesi «da verificare caso per caso, nella quale il titolare del sito consenta comunque agli utenti l'accesso a contenuti o servizi equivalenti senza richiesta di consenso all'uso dei *cookie* o di altri tracciatori». Inoltre, la scelta dell'utente relativa ai *cookie* dovrà essere registrata e non più sollecitata, a meno che non mutino significativamente le condizioni del trattamento, sia impossibile sapere se un *cookie* sia già stato memorizzato nel dispositivo, siano trascorsi almeno 6 mesi. Ritiene infatti il Garante che la ripresentazione del *banner* per la richiesta del consenso agli utenti ad ogni nuovo accesso sia una misura ridondante ed invasiva, che non trova ragione negli obblighi di legge. Resta in ogni caso fermo il diritto degli utenti di revocare in qualsiasi momento il consenso precedentemente prestato. Con questo Provvedimento il Garante si è inoltre espresso esplicitamente contro l'uso dell'interesse legittimo come fondamento per l'uso dei *cookie* e di altri strumenti di tracciamento. Fermo restando che viene ribadito che il consenso debba essere dato in modo "granulare", desta qualche perplessità la previsione di un comando (contenuto nel *banner*) per accettare «tutti i *cookie* o altre tecniche di tracciamento», fermo il rinvio ad altra area nella quale poter scegliere in modo analitico le funzionalità. Il Garante auspica che si arrivi presto ad una codifica universalmente accettata dei *cookie* che consenta di distinguere in maniera oggettiva i *cookie* tecnici da quelli analitici o da quelli di profilazione.

[45] Infatti, la mancanza di opzioni impedisce che il consenso si possa dire dato liberamente. Sui *cookie wall* si v. più ampiamente *supra*, nota 35.

[46] Si veda a riguardo l'avviso datato 26 novembre 2020 sul sito del Garante.

E assegna ai titolari dei siti 6 mesi di tempo per adeguarsi ai principi delle nuove Linee guida.

Quanto alle azioni per le violazioni delle regole sul trattamento dei dati personali sono certo importanti le azioni individuali ma probabilmente ancora di più quelle collettive dato che il singolo interessato potrebbe non procedere a far valere i suoi diritti in giudizio. Accanto a queste ultime è di rilievo il ruolo del Garante per la protezione dei dati personali attraverso la procedura d'urgenza di cui all'art. 66 del Reg. 2016/679 che prevede che, in circostanze eccezionali, qualora ritenga che urga intervenire per proteggere i diritti e le libertà degli interessati, un'autorità di controllo può adottare immediatamente misure provvisorie intese a produrre effetti giuridici nel proprio territorio.

Il Reg. 2016/679 si occupa delle sanzioni per il mancato rispetto della disciplina di protezione dei dati personali agli artt. 77 ss. prevedendo che se l'interessato ritenga che il trattamento che lo riguarda violi il Regolamento ha innanzitutto il diritto di proporre reclamo davanti ad un'autorità di controllo nello Stato membro in cui risiede abitualmente (oppure in cui lavora, oppure in cui si è verificata la presunta violazione)[47]. E tanto, fatto salvo ogni altro ricorso amministrativo o giurisdizionale. L'art. 79 prevede che ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del Regolamento siano stati violati a seguito di un trattamento dei suoi dati personali.

L'interessato ha inoltre il diritto di dare mandato a proporre il reclamo per suo conto e di chiedere per suo conto il risarcimento del danno di cui all'art. 82 ad un organismo o ad un'associazione senza scopo di lucro i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali. L'art. 82 prevede che chiunque subisca un danno «materiale o immateriale» causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Sono previste inoltre sanzioni amministrative pecuniarie che ogni autorità amministrativa di controllo può infliggere a titolari e responsabili che violino varie disposizioni del Regolamento. La violazione è reputata più grave, e di conseguenza più grave è la sanzione, quando siano violati i principi base del trattamento, comprese le condizioni relative al consenso (di cui agli artt. 5, 6, 7 e 9) e i diritti degli interessati a norma degli articoli da 12 a 22 (compreso tra gli altri quindi l'articolo che regola l'informativa). In tali casi più gravi la sanzione amministrativa pecuniaria arriva fino a 20.000.000 di euro o, per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente, se superiore. Altrettanto è previsto per il caso di inosservanza di un ordine da parte dell'autorità di controllo (di cui all'art. 58, par. 2). In ogni caso, le sanzioni pecuniarie irrogate devono essere effettive, proporzionate e dissuasive.

Il 21 maggio 2021 è entrata in vigore anche la nuova disciplina della *class action* disciplinata al codice di procedura civile agli artt. 840 *bis* ss. che va a sostituire, con norme aventi ambito di applicazione più generale, e non riservate ai soli consumatori, le precedenti norme sull'azione di classe date dal codice del consumo agli artt. 140 *bis* ss., che sono stati abrogati. La nuova azione di classe offre la possibilità di tutelare i diritti individuali omogenei sia attraverso un'organizzazione o un'associazione senza scopo di lucro - i cui obiettivi statutari comprendano la tutela dei diritti in questione - oppure su azione di ciascun componente della classe. L'azione è diretta nei confronti dell'autore della condotta lesiva per l'accertamento della sua responsabilità, e per la condanna al risarcimento del danno e alle restituzioni.

4. Recenti decisioni sull'impiego dei *cookie* ed evoluzione delle pratiche diffuse sul mercato.

[47] Contro tale reclamo è possibile il ricorso giurisdizionale, fatto salvo ogni altro ricorso amministrativo o extragiudiziale (art. 78).

Sull'applicazione della disciplina del trattamento dei dati personali alle pratiche di impiego dei *cookie* sono intervenute anche importanti pronunce della Corte di giustizia dell'Unione europea e di autorità nazionali che si sono occupate di casi aventi ad oggetto pratiche di utilizzo dei *cookie* non in linea con il Regolamento 2016/679.

Nel caso *Planet 49* la Corte di giustizia ha affermato che l'unica forma di consenso valido per il trattamento dei dati dell'utente è il consenso espresso, cioè il consenso dato in maniera attiva - ad esempio dato selezionando una casella - e in maniera specifica. Ciò da cui discende che, salvo che per i *cookie* strettamente necessari, è vietata la preselezione delle caselle per esprimere il consenso all'utilizzazione dei *cookie*. L'operatore è inoltre tenuto ad informare gli utilizzatori/interessati quanto alla durata della permanenza dei *cookie* sul suo sito internet, dato che anche questo profilo costituisce una specifica modalità di trattamento dei dati personali. È tenuto anche ad informarli se soggetti terzi hanno o meno accesso ai dati dell'utilizzatore (interessato), ciò che si qualifica come un'ulteriore modalità di trattamento dei dati personali[48]. A tale decisione ha fatto seguito in Germania la sentenza del BGH del maggio 2020 che ribadisce la necessità del consenso attivo per i *cookie* non funzionali[49].

Altra applicazione piuttosto recente concerne un caso spagnolo relativo all'impresa Vueling su cui è intervenuta una pronuncia dell'Autorità garante per la *privacy* spagnola. Rispetto alla pratica secondo cui la Vueling informava gli utenti che il consenso all'operatività dei *cookie* era da esprimersi tramite il *browser* utilizzato dall'utente, il Garante spagnolo ha rilevato tale procedura non consentiva all'interessato di esprimere un consenso specifico per singole tipologie di *cookie*. L'operatore è stato quindi sanzionato per la pratica di non aver fornito la possibilità di rifiutare i *cookie* in quanto la possibilità di disabilitazione era data attraverso configurazione del *browser*. Ed inoltre per le ulteriori pratiche della richiesta del consenso in blocco per tutti i *cookie*, mancando a riguardo un consenso realmente informato, e della previsione del consenso implicito con la prosecuzione della navigazione sul sito. La Vueling è stata sanzionata con una sanzione di 30.000 euro (poi ridotta a 18.000)[50].

Più casi giunti davanti all'autorità garante francese (Vanity Fair, Allocine.fr, eCommerce Cdiscount) sono stati posti in questione per una pratica denominata sotto l'espressione di "falso consenso". Tale pratica prevedeva l'utilizzo di un servizio di *standard* informatici per la gestione dei *cookie* che andava a trasformare un consenso negato dall'utente in un consenso manifestato[51].

Nel marzo 2020 l'Autorità garante francese (CNIL) ha sanzionato il motore di ricerca Google (Google LLC e Google Ireland) con una sanzione pecuniaria di 100 milioni di euro in quanto non forniva agli utenti alcuna informazione quanto alla presenza di *cookie* né segnalava la possibilità di rifiutarli[52]. L'ammontare della sanzione era giustificato dalla gravità della triplice violazione dell'art. 82 della legge francese sulla protezione dei dati personali, dal

---

[48] Corte giust. Ue, 1° ottobre 2019, C-673/17, *Bundesverband der Verbrauchenzentrale und Verbraucherverbände – Verbraucherzentrale Bundesverband eV c. Planet49*.

[49] BGH, 28 maggio 2020, case no. I ZR 7/16, *Planet 49*. Come si può indirettamente rilevare rimane in parte non ben definito sin dove si estenda l'ambito dei *cookie* cui dare la qualifica di *cookie* tecnici, per i quali non sarebbe necessario il consenso dell'interessato. Se la categoria ricomprenda solo quelli strettamente necessari per la navigazione, secondo l'interpretazione più restrittiva, o se la categoria sia da intendersi in modo un po' più ampio. E in tal senso anche il Provvedimento n. 231 del 10 giugno 2021 del nostro Garante della *privacy* che ha ricompreso in questa categoria i *cookie* analitici di rilievo statistico. V. a tale riguardo *supra*, par. 3.

[50] Autorità garante *privacy* Spagna, Resolucion R/00499/2019, 10 ottobre 2019, *Vueling*.

[51] CNIL, casi C-20/19, C-21/19, C-22/19.

[52] L'Autorità aveva rilevato che quando un utente arrivava su google.fr i *cookie* venivano depositati automaticamente sul suo computer senza alcuna azione da parte sua e che molti di questi *cookie* erano usati a scopi pubblicitari. Nella pagina raggiunta l'utente trovava sul *banner* informativo la scritta "Promemoria sulla *privacy* di Google", i "pulsanti" intitolati "Ricordamelo dopo", e "Visualizza ora", che tuttavia non aggiungevano informazioni utili ad illustrare l'uso dei *cookie*. V. rif. cit. alla nota seg.

numero degli interessati coinvolti, ossia quasi cinquanta milioni di utenti, e dai notevoli profitti che le due società avevano tratto dai ricavi pubblicitari generati indirettamente dai dati raccolti dai *cookie* traccianti. Nel settembre 2020 l'Autorità dava atto che a seguito di un aggiornamento da parte di Google non venivano più rilasciati automaticamente *cookie* pubblicitari appena l'utente arrivava sulla pagina di Google, tuttavia il nuovo *banner* informativo non risultava soddisfacente in quanto non permetteva ancora di comprendere le finalità di utilizzazione dei *cookie*, né permetteva di rifiutarli[53]. Nel contempo, la stessa Autorità ha sanzionato anche Amazon (Amazon Europe Core) con una sanzione pecuniaria di 35 milioni di euro per un comportamento analogo – ossia per mancata richiesta del consenso dell'interessato - rispetto all'uso dei *cookie*. Le informazioni fornite da Amazon non erano né chiare né complete: il *banner* informativo prevedeva che "Utilizzando questo sito si accetta il nostro uso dei *cookie* per offrire e migliorare i nostri servizi" cui era accluso un pulsante "Per saperne di più". La descrizione generica del *banner* sugli scopi di tutti i *cookie* non era sufficiente a dare la possibilità all'utente di comprendere che i *cookie* avevano lo scopo principale di far visualizzare pubblicità personalizzata e tale *banner* non indicava all'utente il diritto di rifiutare i *cookie* e i mezzi disponibili a tale scopo. Come per il caso precedente la sanzione veniva giustificata in base all'art. 82 della legge francese, alla circostanza che la personalizzazione degli annunci resa possibile grazie ai *cookie* aumentava notevolmente la visibilità dei prodotti, e che gli interessati coinvolti erano milioni di persone. Ancora, sempre allo stesso modo del caso precedente il nuovo *banner* informativo non consentiva agli utenti di comprendere che i *cookie* venivano usati principalmente a scopi pubblicitari e che fosse possibile rifiutare i *cookie*[54].

Di recente si sono registrate pratiche di trattamento dei dati personali attraverso i *cookie* che gli operatori fondano non sul consenso dell'utente/interessato ma sul legittimo interesse dell'operatore. In questi casi l'operatore utilizza previsioni che si traggono dal considerando 47 e dall'art. 6.1 lett. *f* del Reg. 2016/679 per giustificare il trattamento di dati personali in base al suo legittimo interesse[55], cosicché se l'utente non deseleziona la casella del *banner* preimpostata sulla sussistenza di un legittimo interesse dell'operatore – o se, secondo una diversa pratica, acconsente al trattamento in base al legittimo interesse - il trattamento dei dati avviene in base a quest'ultimo[56]. Su tali pratiche fondate sul legittimo interesse si è espresso da ultimo in senso negativo il Provvedimento del Garante della privacy n. 231 del giugno 2021, come si è visto sopra al paragrafo 3.

5. Uso dei *cookie* e disciplina di tutela del consumatore.

Nei casi in cui l'utente del sito internet sia un consumatore, alle pratiche che gli operatori adottano per l'uso dei *cookie* al fine del trattamento dei dati personali degli utenti/interessati risultano applicabili, oltre alla disciplina del trattamento dei dati personali, anche le discipline di tutela del consumatore.

---

[53] Le informazioni su questo caso sono tratte da www.privacy.it, *Cookie traccianti, dal CNIL sanzioni multimilionarie a Google ed Amazon*, 10 dicembre 2020.

[54] Le informazioni su questo caso sono tratte da www.privacy.it, *Cookie traccianti, dal CNIL sanzioni multimilionarie a Google ed Amazon*, cit.

[55] Ricorda ad es. M.C. MENEGHETTI, *Consenso* bis*: la Corte di Giustizia torna sui requisiti di un valido consenso* privacy, cit., che il legittimo interesse è uno dei cinque presupposti alternativi al consenso per il trattamento dei dati personali (gli altri sono adempimento contrattuale o normativo, interesse pubblico, tutela degli interessi vitali).

[56] Nel concreto a volte accade che gli operatori inseriscano nel *banner* una casella, da selezionare da parte dell'utente, per l'espressione del consenso al trattamento dei dati personali per la singola tipologia di *cookie*, ed un'altra casella per la stessa tipologia di *cookie* già preselezionata a significare il legittimo interesse dell'operatore a trattare i dati personali dell'utente. Tali pratiche vengono poste in essere anche, per esempio, per *cookie* di profilazione.

Si pensi alla disciplina delle clausole vessatorie con particolare riguardo alle clausole dell'informativa, sindacabili rispetto al canone della trasparenza sia quanto al loro contenuto e alla loro formulazione letterale che quanto al loro aspetto grafico[57]. La comprensibilità e la chiarezza della formulazione dell'informativa che accompagna la richiesta del consenso all'interessato è sicuramente un profilo critico alla luce di tale disciplina. Anche a questo riguardo potrebbero prestarsi ad essere di utilità gli sviluppi e le applicazioni di *legal design* di cui si è detto sopra. Per i rapporti tra la disciplina delle clausole vessatorie nei contratti del consumatore di cui alla dir. 93/13 e la disciplina del trattamento dei dati personali è di interesse il considerando 42 del Reg. 2016/679 che richiama la dir. 93/13 nel senso che «in conformità della dir. 93/13 (…) è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e che non contenga clausole abusive». Considerando che peraltro non opera distinzioni tra utenti/interessati consumatori e non consumatori, e quindi parrebbe suggerire anche un ampliamento del controllo di trasparenza al di là dei contratti del consumatore[58].

Ai testi e alle grafiche utilizzate dall'operatore è applicabile inoltre la disciplina delle pratiche commerciali scorrette, quali pratiche adottate dall'operatore nel contesto della propria attività commerciale che possono indurre il consumatore ad adottare un comportamento economico che non avrebbe altrimenti adottato (art. 20 c.cons.). Nella gran parte dei casi, infatti, le pratiche di trattamento dei dati personali adottate dagli operatori hanno una portata di tipo economico, obiettivi e ricadute economicamente valutabili (in modo diretto per la propria attività economica, e attraverso la cessione dei dati a terzi a volte indiretto), e in questa prospettiva si rivolgono al consumatore influenzandone i comportamenti. Anche il comportamento del consumatore assume peraltro in sé una portata economicamente valutabile in quanto sui siti che il consumatore raggiunge, e che trattano i suoi dati personali, questi acquista, assume informazioni utili all'acquisto o informazioni che possono avere diretto o indiretto valore economico.

La disciplina delle pratiche commerciali scorrette può venire in considerazione sotto diversi profili. Come si è visto sopra, al paragrafo 2, si trovano impiegate pratiche di richiesta del consenso precedute da un'informativa sul trattamento dei dati personali e i suoi scopi formulate in modo poco chiaro quanto al testo impiegato e/o alla grafica impiegata. Si trovano inoltre impiegate avvertenze preliminari al trattamento dei dati attraverso i *cookie* dal significato ingannevole, come ad esempio espressioni secondo le quali "l'operatore ha massima cura del dati personali dell'utente", e per questo motivo procede al trattamento di dati dell'utente, che poi vengono raccolti a vari scopi, anche di profilazione. Questi sono appunto messaggi ingannevoli per l'utente di internet che potrebbe essere indotto ad un comportamento avente una portata economica diverso da quello che avrebbe altrimenti assunto, secondo la definizione impiegata dalla disciplina delle pratiche commerciali

---

[57] La c.d. *privacy policy* dell'operatore, preceduta dalla relativa informativa, si compone di determinazioni che regolano il trattamento dei dati personali che si prestano ad essere qualificate come clausole contrattuali. LOOS e LUZAK, *Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers*, in *Amsterdam Law School Legal Studies Research Paper*, No. 2015-01 (ora in *Journ. Cons. Policy*, 2015), p. 5. La natura contrattuale delle condizioni delle *privacy policy* è chiara nelle impostazioni in cui, nello studio dei rapporti con i consumatori, l'intera area della regolazione della *privacy* viene sussunta nella disciplina dei contratti del consumatore, BEN-SHAHAR e STRAHILEVITZ, *Contracting over Privacy: Introduction*, in 45 *Journal of Legal Studies* S1, 2016, p. 51 ss. Con le dir. 2019/770 e dir. 2019/771 UE questo è emerso in maniera espressa.

[58] Tanto richiama anche la questione se le determinazioni dell'informativa possano essere qualificate come clausole contrattuali nel senso che il rapporto tra l'utente e il gestore del sito sia da ritenersi un rapporto di natura contrattuale avente ad oggetto se non altro utilità come le informazioni che l'utente assume dal sito internet.

scorrette. Si trova poi da parte degli operatori il ricorso a *banner* per la richiesta del consenso al trattamento dei dati personali che occupano fisicamente buona parte della pagina *web*, sollecitando il fastidio dell'utente, e l'impressione di non poter procedere nella navigazione se non accordi il consenso all'utilizzazione dei *cookie*. In questo caso la pratica commerciale scorretta pare potersi qualificare come una pratica di natura aggressiva (art. 24 c.cons.).

In via più generale, come hanno affermato provvedimenti dell'Autorità garante per la concorrenza e il mercato e pronunce giurisprudenziali deve essere chiaro per l'utente/interessato – quando questo corrisponda al caso, quindi soprattutto per i *cookie* analitici e di profilazione – se e quando i dati vengono trattati dagli operatori per finalità commerciali, diversamente l'interessato non è in grado di dare un consenso consapevole al trattamento dei suoi dati. Le pratiche di trattamento dei dati personali che non rivelino fin dall'inizio all'utente le proprie finalità e l'impiego dei dati a scopo commerciale, contrariamente a quanto realizzato dall'operatore, sono state sanzionate come pratiche commerciali scorrette[59].

6. Uso dei *cookie* e tutela dei diritti fondamentali della persona diversi dal diritto alla protezione dei dati personali.

Altro aspetto da prendere in considerazione relativamente alle pratiche di trattamento dei dati personali attraverso i *cookie* è che queste potrebbero importare la lesione di diritti fondamentali come quelli all'informazione e all'educazione. Si pensi ai casi in cui il consenso dell'utente venga richiesto nei fatti in maniera obbligata per accedere a contenuti che non sarebbero disponibili altrove, come può accadere per i siti internet istituzionali, di organizzazioni di carattere pubblico o anche privato quando su questi siti si trovano informazioni non disponibili o non disponibili facilmente altrove. Questo quando il mancato consenso ai *cookie* impedisca la navigazione sul sito (*cookie wall*)[60], oppure quando vengano impiegate caselle preselezionate in maniera obbligata e l'utente decida di non procedere nella navigazione per non consentire il trattamento dei propri dati personali.

Si pensi inoltre alle pratiche di "falso consenso" di cui si è detto sopra, al paragrafo 4, nelle quali si potrebbe intravvedere, oltre alla lesione del diritto sui propri dati personali, la violazione della libera manifestazione del pensiero.

A ben riflettere, ad ogni modo, parrebbe che anche la richiesta di dati a mezzo di *cookie* impiegata di fatto quale "chiave di accesso" pure ad un sito meramente privato, con informazioni reperibili altrove, come attraverso l'impiego di pratiche di *cookie wall*, potrebbe essere lesivo di diritti dell'utente potenziale del sito internet, come il diritto all'informazione[61]. Questo in quanto se in tale caso si può pensare legittimo vietare o rendere più elaborato l'accesso ad un sito che non contenga informazioni di rilievo che non sarebbero disponibili altrove, tutto ciò parrebbe potersi realizzare in maniera più riconoscibile e quindi più rispettosa dei diritti della persona soltanto in maniera che sia chiaramente riconoscibile per l'utente, ad esempio chiedendo la registrazione al sito per ottenere l'accesso. Con il trattamento dei suoi dati attraverso i *cookie* l'utente potrebbe invece non percepire in maniera chiara che l'accesso al sito e alle informazioni che qui si trovano richiede in sostanza come corrispettivo la cessione dei suoi dati personali.

Conclusioni.

[59] Si veda la decisione della nostra Autorità garante per la concorrenza e il mercato del 2018 relativa alle pratiche impiegate da Facebook e la successiva pronuncia di Tar Lazio, 20 gennaio 2020.

[60] V. a riguardo *supra*, par. 2, e qui indicazioni sui *cookie wall*, a nota 35.

[61] Tanto dipende anche dal ruolo che si riconosca a internet e alla navigazione sui siti internet, su cui ci si soffermerà *infra*, nel paragrafo successivo.

Ci si può soffermare a meditare su quali siano le possibili strade praticabili di fronte ad un uso dei *cookie* che in ogni caso, come si è visto sopra nel paragrafo 2, pure quando sia osservante delle prescrizioni di tutela dei dati personali (ciò che si è visto non corrisponde alle pratiche mediamente diffuse sul mercato) e delle altre discipline che possono essere interessate, crea per l'utente una situazione con a quale regolarmente ha difficoltà a misurarsi.

Date le problematiche che si riscontrano rispetto alla tutela dei dati personali degli interessati – e ci si riferisce all'utilizzo di *banner* con informativa di primo e secondo livello con informazioni non sempre facilmente comprensibili dagli utenti, a meno che non si tratti di utenti particolarmente esperti e/o sensibili al fenomeno –, parrebbe necessario riflettere su una regolazione dei *cookie* che per il futuro riveda la piena legittimità quanto meno dei *cookie* di profilazione utilizzati dalle imprese a scopo di *marketing* e allo scopo di successiva cessione ai terzi di dati personali (insidiosi in quanto l'utente non riesce a seguire il percorso dei dati). Le pratiche di utilizzo di tali *cookie* pongono l'accesso e la navigazione sui siti internet in qualche modo come consentita dietro il corrispettivo dell'acquisizione dei dati personali degli utenti, ciò che non costituisce un problema in sé e per sé, ma quando si rifletta sulle funzioni che si riconoscano al mezzo internet nella realtà contemporanea, come si farà qui più avanti.

L'impostazione della Proposta del nuovo Regolamento *e-privacy* sopra citata non pare molto di supporto ad introdurre novità nella regolazione dell'utilizzo dei *cookie*. Piuttosto mette in luce le difficoltà strutturali sopra enunciate, anche se limitatamente agli utenti che siano anche consumatori, il Documento del BEUC "*EU Consumer Protection 2.0 – Structural asymmetries in digital consumer market*" di cui si è detto sopra nel paragrafo 2.

Quanto alla funzione che assume internet nella nostra società, ci si deve soffermare a riflettere se vi si riconosca una esclusiva funzione di mercato o una funzione di *media* informativo, e a volte anche educativo degli utenti e dei cittadini. Nelle riflessioni sull'accesso ad internet si è giunti diffusamente alla conclusione, appunto, che oggi l'accesso ad internet ha una funzione informativa, di realizzazione del diritto del cittadino all'informazione, ed anzi tante volte anche una funzione educativa del cittadino[62]. Con riguardo alle funzioni di carattere informativo generale che internet può assolvere, si pensi per esempio alla circostanza che oggi le informazioni non finanziarie che le imprese di grandi dimensioni sono tenute a rendere note al pubblico (a seguito della dir. 2014/95 Ue) vengono pubblicate sui loro siti internet[63]. Le imprese che sono tenute a rispettare lo *Anti-slavery Protection Act* in vigore nel Regno Unito dal 2015 devono pubblicare sui loro siti internet i dati relativi alle

---

62 V. a riguardo VALLE, *Il contratto e la realizzazione dei diritti della persona*, Torino, Giappichelli, 2020, pp. 251-252. RODOTÀ, *La cittadinanza digitale*, in *Il mondo nella rete*, Roma-Bari, 2014, p. 13 ss., che vede il punto di avvio della riflessione su un diritto di accesso ad internet – il cui riconoscimento ritiene peraltro necessario (ID., *Epilogo*, in *Il mondo nella rete*, cit., p. 72) – nella prospettiva secondo la quale si tratta «non solo [di un] diritto a essere tecnicamente connessi alla rete, bensì [della] espressione di un diverso modo d'essere della persona nel mondo». Riprende il punto FROSINI, *Il diritto di accesso a internet*, in *Diritti e libertà in Internet*, a cura di Frosini, Pollicino, Apa, Bassini, Milano, 2017, pp. 43, 45, citando RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p. 384, nell'affermare che si tratti «non tanto e non solo [del] diritto a essere tecnicamente connessi alla rete Internet ma piuttosto [di un] diverso modo di essere della persona nel mondo e (…) effetto di una nuova e diversa distribuzione del potere sociale. Sempre più l'accesso alla rete Internet, e lo svolgimento su di essa di attività, costituisce il modo con il quale il soggetto si relaziona con i pubblici poteri, e quindi esercita i suoi diritti di cittadinanza. Oggi la cittadinanza è digitale». E che internet è «un servizio universale, che le istituzioni nazionali devono garantire ai loro cittadini attraverso investimento statali, politiche sociali e educative, scelte di spesa pubblica».

63 Si consideri che la pratica di elaborare comunicazioni non finanziarie pare andare diffondendosi anche presso le imprese non soggette ad obbligo, come le imprese di medie e piccole dimensioni. Le imprese sono e saranno nel prossimo futuro interessate a diffondere tali informazioni sui loro siti internet come mezzo di attrazione della clientela e di affidabilità per i *partner* commerciali, nonché come mezzo per ottenere l'accesso al credito.

loro azioni in linea con tale legge[64]. Si veda inoltre l'art. 3 del Reg. 2020/852 che prevede che i partecipanti ai mercati finanziari e i consulenti finanziari pubblichino sui loro siti *web* le rispettive politiche sull'integrazione dei rischi di sostenibilità nei processi decisionali relativi agli investimenti e nelle consulenze in materia di investimenti o di assicurazioni. In ragione di questa funzione che la navigazione su internet assolve, pare che l'adozione da parte delle imprese di *cookie* che vadano oltre ai *cookie* necessari per la navigazione e a quelli che servono ad assicurare certe funzioni all'utenza sia una pratica sbilanciata a carico degli utenti che accedono ai siti, e non in linea con il significato che la navigazione sulla rete internet assume nella realtà contemporanea. L'acquisizione di dati personali dell'utenza a scopi di programmazione dell'attività degli operatori e a scopi di introiti pubblicitari dovrebbe essere assegnata ad altri strumenti rispetto al mero accesso al sito internet, attraverso l'acquisizione di un rapporto più stretto con gli utenti, che potrebbe passare ad esempio attraverso l'accesso al sito con dati identificativi – che rendono sotto questo profilo più chiara all'utente la relazione con il sito - e l'utilizzo di *applications* (App). Avendo ad ogni modo presente che, se tali ultime pratiche indicate fanno salva la funzione informativa, ed a volte educativa, della navigazione su internet, esse possono comunque presentare a loro volta problematiche, anche penetranti, di rispetto della posizione e dei diritti degli utenti sulle quali è opportuno pure riflettere in vista della regolazione che si vuole vedere realizzata nel prossimo futuro[65].

Indipendentemente da profili più direttamente legati all'applicazione normativa delle discipline di tutela dei dati personali, pare aprire a nuove pratiche di impiego dei *cookie* l'annunciata revisione delle relative *policy* da parte dei motori di ricerca (che comunque fa seguito a più sanzioni delle pratiche da questi adottate nel trattamento dei dati degli utenti), in particolare con riguardo alla rinuncia ai *cookie* di terze parti (i dati degli utenti sarebbero quindi trattenuti in proprio dall'operatore)[66].

Si può pensare quindi che il ricorso all'utilizzo dei *cookie*, nonostante le recenti pronunce giurisprudenziali di rilievo e le altrettanto recenti guide e pareri delle autorità di protezione dei dati personali, compresa quella dello *European Data Protection Board*, presenterà nel futuro nuove prospettive e aprirà nuovi e diversi quesiti relativamente alla sua disciplina giuridica.

---

[64] Nel 2015 nel Regno Unito è stato adottato il *Modern Slavery Act* che prevede che le imprese che rientrano nella previsione dell'art. 54 dell'*Act* devono esibire uno "*Slavery and human trafficking statement*" annuale e pubblico approvato dal loro consiglio di amministrazione che sia raggiungibile da un *link* evidente sulla *homepage* dell'impresa.

[65] ZUBOFF, *Il capitalismo della sorveglianza*, trad. it. Bassotti, 2019 (pubblicazione originale *The Age of Surveillance Capiytalism*, 2019), Roma, Luiss University Press, p. 247 ss.

[66] Google ha recentemente annunciato che rinvierà il blocco dei *cookie* di terzi su Chrome al 2023, secondo la notizia tratta da *hdblog* e datata 24 giugno 2021. Nel 2017 era anche stato lanciato in Italia un motore di ricerca etico quanto all'utilizzo dei *cookie*, Qwant, che non traccia le attività degli utenti e non li profila a scopo pubblicitario.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Online platforms: new vulnerabilities to be addressed in the European legal framework. Platform to business user relations.

ANDREA D'ALESSIO
Ph.D. at the University of Teramo
Lawyer

Abstract

Online platforms play a significant role in facilitating the exchange of goods and services, operating as market makers. Their intermediation function is carried out through the conclusion of a series of unilaterally determined contracts, in which business users have a specific vulnerable position. Therefore, the need to ensure the growth of this phenomenon led to the adoption of Reg. (EU) No. 1150/2019, "On promoting fairness and transparency for business users of online intermediation services". The new legal framework seeks to address commercial users' vulnerabilities related to asymmetry of knowledge and bargaining power. The paper aims to analyze this Regulation its problematic aspects.

Keywords: online platforms - B2B contracts - new vulnerabilities - unfair commercial practices.

Summary: Introduction. – 1. Matter and scope. – 2. Terms and conditions. – 3. Rules for contractual relations. – 4. Alternative dispute resolution. – Conclusions.

Introduction.

Online platforms[1] are now a significant reality, and their strategic role has been highlighted by the difficulties associated with the Covid19 pandemic. In a world that suddenly turns out to be fragile, stuck and distant, the possibilities granted by the collaborative economy, and its digital and virus-free marketplace, become crucial. Although this new paradigm could be considered largely positive, it implies some concerns.

First, it is necessary to consider that economic studies have suggested a particular role for these platforms as market makers[2]. In fact, they usually act as a conjunction between

[1] For a definition of platform see A Wiewiorowska-Domagalska, 'Online Platforms: How to Adapt Regulatory Framework to the Digital Age', Briefing of the European Parliament, 2017, 2: «Taking a very general, economic approach, online platforms mean two-sided markets, namely digital infrastructure that allows interactions and helps fulfil the interests of two groups of users: suppliers and customers».
Among the huge number of contribution on the topic of legal framework applying to online platforms see G Cassano, I P Cimino, 'Contratto via Internet e tutela della parte debole' (2002) *Contratti*, 870; M Colangelo, V Zeno-Zencovich, 'La intermediazione on-line e la disciplina della concorrenza: I servizi di viaggio, soggiorno e svago' (2015) 1 *Dir.Inform.*, 43; A De Franceschi (ed.), *European Contract Law and the Digital Single Market*, (2016) Cambridge; A Quarta, 'Il ruolo delle piattaforme digitali nell'economia collaborativa' (2017) *Contr.impr.Eur.*, 554–571; C Twigg-Flesner, 'The EU's Proposals for Regulating B2B Relationships on online platforms–Transparency, Fairness and Beyond' (2018) 6 *EuCML*, 222; J Campos Carvalho, 'Online Platforms: Concept, Role in the Conclusion of Contracts and Current Legal Framework in Europe' (2020) 12 *Cuad.Der.Trans.*, 867.
[2] See G Smorto, *Critical Assessment of European Agenda for the Collaborative Economy, on behalf of European Parliament. In-Depth Analysis for the IMCO Committee. Bruxelles: Policy Department A - European Parliament C.* (2017), consultable at
http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/595361/IPOL_IDA(2016)595361_EN.pdf

suppliers and customers by circumventing the material and geographical barriers that may hinder an analogic contact. Platforms overcome these limitations by creating a new environment for commercial relationships on the web, in which they act, though not always[3], as intermediaries between different parties interested in the exchange of goods and services[4].

In addition, platforms can create different types of connections, corresponding to the wide variety of interests that seek a channel on the web. It is possible to classify these relationships on a subjective level, given the different roles played. The parties can be either consumers interested in sharing some underused personal good, or traders with the purpose of offering goods or services to both consumers and other businesses. Therefore, the whole spectrum of contractual relationships can originate from platforms. The first type of them responds to the C2C model and can be defined as a part of the sharing economy, i.e. a model in which strict property rights are softened in a common use perspective[5]; on the other hand, online platforms can also be involved in the establishment of more classic B2B and B2C relationships and in these cases the new phenomenon is called collective economy.

Both new paradigms show criticalities from the legal point of view: the former could be used as a convenient mask for ordinary market relations, avoiding the application of tax or labor laws; the latter emphasizes the need for consumer protection, as in the case of personal data, but can also show the emergence of new types of vulnerabilities[6].

The latter perspective is particularly interesting for legal design because of the need to protect subjects who, on an ordinary and entirely analogical level, have been considered strong players in the Market, i.e. economic operators.

In fact, suppliers interested in extending or basing their business on the wide opportunities disclosed by online platforms are involved in contractual relationships with these intermediaries, which can be characterized by many aspects of disparity.

(accessed: 29th June 2020); A Quarta, 'Il ruolo delle piattaforme digitali' (n 1) 555; C Twigg-Flesner, 'The European proposal' (n 1) 224.

[3] Platforms often act as suppliers of good and services in addition to a genuine intermediation role. Other times, they present themselves to customers as intermediaries even though they act exclusively as suppliers. See A Wiewiorowska-Domagalska, *Online Platforms* (n 1) 6; A Quarta, 'Il ruolo delle piattaforme digitali' (n 1) 558; J Campos Carvalho, 'Online Platforms' (n 1) 867. This criticism is also clarified in point 43 of Conclusion by Adv.

[4] The first implication on a contractual level is represented by the multiplication of contractual relationships in the circulation of goods and services: one between Platforms and suppliers, another between platforms and customers, and the last between suppliers and customers. See J Campos Carvalho, 'Online Platforms' (n 1) 866.

[5] On the topic see Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2016) 356 final, 'A European agenda for the collaborative economy'.
In doctrine, e.g., T. Bonini, G. Smorto (eds.), *Shareable! L'economia della condivisione*, (Edizioni di Comunità 2017); R Botsman, R Rogers, 'What's Mine is Yours' (2nd edn, Collins 2011); R. Belk, 'Sharing', (2010) *J.Consum.*, 36. Moreover, J Campos Carvalho, 'Online Platforms' (n 1) 865, recognizes sharing economy as part of the online platform phenomenon on a contractual level.

[6] See E Bacciardi, 'Contratti telematici e diritto di recesso' (2010) 4 *Contratti*, 381-391; F Lazzarelli, *L'equilibrio contrattuale nelle forniture di sistemi informatici* (ESI 2012); F Galli, 'La nullità della clausola MFN nei contratti tra agenzie di intermediazione ed imprese alberghiere'(2018) 6 *Nuove leg. civ. comm.*, 1387.

Table 0.3 Potential negative trading practices in different stages of commercial relationship

Thematic field	Pre-contractual period	Contract formation	Contract performance	Contract expiry/ termination & post-contractual period
1. Setting the terms and conditions	• Refusal to negotiate; • Lack of clarity on the full T&C.	• Non-negotiability of changes; • Lack of clarity and vague language of T&C.	• Unilateral changes; • Unilateral interpretation of T&C; • Lack of or very short-term prior notice about changes; • Continuation of use as a presumption of acceptance of changes.	• Unilateral termination.
2. Search and ranking	• Transparency of search criteria.	• Lack of transparency regarding search, ranking and reference functions.	• Provision of information on changes to ranking algorithms; • Use of alternative tool to present offers.	
3. Access to the platform	• Eligibility to access the platform.	• Lack of transparency of rules related to delisting of products, suspension of account and termination of accounts.	• Lack of information on delisting of products of services; • Lack of information on temporary suspension of an account; • Lack of information on actions required for relisting of products/services or re-instating of an account.	• Lack of information on termination.
4. Platforms competing with business users or limiting options		• Parity clauses (price and non-price related); • Limitations of choice of auxiliary services;	• Platforms favouring own products; • Lack of explanation of operational decisions.	
5. Data access and portability	• Lack of information on policy re data.	• Lack of transparency regarding data access and portability.	• Limited access to data; • Restrictive application of provisions on data access/ sharing and use.	• Retention of data related to business user.
6. Problem solving		• Non-EU jurisdiction and applicable law; • Liability disclaimers; • Lack of penalties for platforms.	• Restrictions on access to redress possibilities.	

Table taken from Final Report of the study *Business-to-Business relations in the online platform environment* written by Ecorys for the European Commission.

Most importantly, commercial users of the platform are often unaware of how their counterpart's algorithm works. Despite its technical nature, this aspect has a fundamental legal implication, as the algorithms' functions are closely linked to the platforms' contractual performance. In particular, the software determines the ranking of each offer, playing a strategic role in the profitable use of the service.

Another critical issue is related to the position of intermediaries in the new environment. As market makers, they can act as arbitrators for the relationships they help create. In doing so, they provide systems that can give clients the opportunity for indirect incidence on the level of benefits to providers, with particular regard to feedback mechanisms[7].

The new position of vulnerability has been considered by the European institutions since 2016[8]. The Commission launched a public consultation highlighting concerns about unfair business practices by online platforms. The most common alleged problems include unfair terms and conditions; platforms refusing market access or unilaterally modifying the conditions for market access; the dual role that platforms may play as intermediaries and suppliers; unfair 'parity' clauses with detrimental effects for the consumer; and lack of transparency.

[7] In two-sided or multi-sided markets platforms consider only one group of parties as profit generator; in a relevant number of cases this role is attributed to customers. See J Campos Carvalho, 'Online Platforms' (n 1) 866–867; S Casabona, 'Intermediazione digitale e composizione delle controversie: dall'Alternative Dispute Resolution all'Alien Dispute Resolution' (2017) 3 *Dir. Informatica*, 497; A Quarta, 'Il ruolo delle piattaforme digitali' (n 1) 565; M Colangelo, V Zeno-Zencovich, 'La intermediazione on-line' (n 1) 43; P Perri, 'Sospensione dell'account del venditore dalla piattaforma eBay a seguito di feedback negativi: profili civilistici e informatico-giuridici', (2011) 7-8 *Giur. mer.*, 1809.

[8] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 25.5.2016 COM(2016) 288 final, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe; Accompanying the document COM(2016) 320 final, SWD(2016) 163 final, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices.

In order to address these issues, the European institutions have introduced the recent Regulation (EU) n. 1150/2019 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services. In this Regulation, they have adopted a legal protection framework that applies, for the first time, to a broad area of B2B relationships, namely those between Platforms and their business users (P2B contracts)[9].

The aim of the paper is to realise a first reading of this protection law.

1. Matter and scope.

In Reg. (EU) 1150/2019, the European institutions sought to address the new challenges of the online marketplace with the aim of ensuring legal certainty[10].

In particular, the Whereas highlight that this objective is crucial for the success of new business models that can exploit the opportunities of platforms. The latter represent fundamental resources for the future development of the internal market, but they may also lead to the emergence of a new form of economic dependence. Indeed, the central position that platforms occupy in online markets could cause a great disparity in bargaining power and knowledge between them and their business users.

Therefore, in order to maximise the positive effects of a fair and equitable online platform environment, the Regulation selects a specific scope.

In particular, the subjective level makes clear the change in the EU's approach to market regulation. In fact, it regulates the relationships between Platforms, intended as providers of intermediation services[11] or «online searching engines», and business users or «corporate website users»[12]. Each of these entities is an economic operator and the regulation represents the European response to the new form of vulnerability.

---

[9] See J Campos Carvalho, 'Online Platforms' (n 1) 874.

[10] See 1st whereas Reg. (EU) n. 1150/2019: « Online intermediation services are key enablers of entrepreneurship and new business models, trade and innovation, which can also improve consumer welfare and which are increasingly used by both the private and public sectors. They offer access to new markets and commercial opportunities allowing undertakings to exploit the benefits of the internal market. They allow consumers in the Union to exploit those benefits, in particular by increasing their choice of goods and services, as well as by contributing to offering competitive pricing online, but they also raise challenges that need to be addressed in order to ensure legal certainty».

[11] This choice ensures the effectiveness of the framework, because it allows a huge number of online operators to be considered as intermediation service providers. In particular, it is not relevant whether the contract between supplier and customer is directly concluded on the supplier's site, because it is only necessary that the supplier can establish an initial contact between the parties. In this sense the Regulation lists in 11th recital some examples, such as online e-commerce market places, online software applications services, like application stores, and online social media services.

[12] Regulation (EU) n. 1150/2019 ignores prosumers, i.e. consumer that operate on online platforms as suppliers. The difficulty of a clear distinction between business operators and prosumers would have advised the assumption of a different approach, such as applying consumer acquis to each contract between platforms and users. See A Wiewiorowska-Domagalska, *Online Platforms* (n 1) 7; A Quarta, 'Il diritto dei consumatori ai tempi della peer economy. Prestatori di servizi e prosumers: primi spunti', (2017) 2 *Europa dir. priv.*, 667-681; M Maugeri, 'Elementi di criticità nell'equiparazione, da parte dell'Aeegsi, dei "prosumer" ai "consumatori" e ai "clienti finali"' (2015) 2 *Nuova giur. civ. comm.*, 406; R. Montinaro, 'Il consumatore nei mercati online: la disciplina del commercio elettronico e delle pratiche commerciali scorrette alla prova dell'evoluzione tecnologica' (eds. A. Catricalà, M.P. Pignalosa) Saggi di diritto dei consumi (2020), 75-113.
The European Court of Justice, in sentence CJEU, cause C-105/17 of 4th October 2018, has indicated a list of criteria for the application of consumer protection rules in the contract between prosumer and consumer. Moreover, the Commission indicated three principal criteria, i.e. frequency of the services, profit-seeking motive and level of turnover in Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2016) 356 final, A European agenda for the collaborative economy.

Moreover, the regulation has a broad scope. In fact, the European intervention refers to two different types of situations and only a part of the regulated relationships, i.e. those in which Platforms act as providers of services and their business[13], is based on a contract. Besides these, the regulation extends its application to another type of relationship that is not considered contractual and takes place between owners of corporate websites and online search engines.

The relationships included in the contractual scheme are characterised by the fact that both parties involved are professionals and their contract is fully referable to the B2B model. Moreover, it can be noted that the company size of the different actors is not taken into account within the framework. Indeed, although the recitals refer to the need for special protection for micro or SMEs[14] operating through an online platform, art. 2(10) makes it clear that the size of the parties is not decisive[15]. On the other hand, the Regulation shows a certain degree of concern for small platforms[16], exempting them from the obligations of Articles 10 and 11.

This objective of protection is also apparent from the territorial scope of the regulation, which consists of all cases where commercial users have «their place of establishment or residence in the Union», notwithstanding the nationality of the providers of intermediary services or online search engines.

The presence of a contract makes it easier for the European institutions to establish a level of protection for these economic operators. On the contrary, in the relations between business website owners and online search engines, which are not governed by the contractual paradigm, the regulation merely obliges providers to grant access and transparency for the most relevant elements of their functioning.

These innovative elements in the subject matter and scope of the regulation are counterbalanced by the classic attention of consumer contracts.

In this sense, even if the regulation does not specifically consider the protection of consumers, there is an indirect focus on them in the area of application. In fact, as indicated in Art. 1(2), it is necessary that platforms are involved in the direct or indirect conclusion of contracts between commercial users and consumers; the regulation does not apply to platforms that create connections between commercial parties. Therefore, for the scope of application of the Regulation, P2B relationships are relevant only if characterised by the

---

13 In this sense the European choice has been considered coherentist. See C Twigg-Flesner, 'The European proposal' (n 1) 231.
A debate concerning the relevance of contractual paradigm in online transactions had been animated in Italian doctrine. See N Irti, 'Scambi senza accordo' (1998) 2 *Riv. trim. dir. proc. civ.*, 347-364; G Oppo, 'Disumanizzazione del contratto?' (1998) 5 *Riv. dir. civ.*, 525 – 533; N Irti, 'È vero ma ... (replica a Giorgio Oppo)' (1999) 2 *Riv. dir. civ.*, 273–278.

14 See 2nd whereas Reg. (EU) n. 1150/2019.

15 In particular, this article refers to the relevance of terms and conditions unilaterally determined by providers of online intermediation services. It states that they have to be «evaluated on the basis of an overall assessment, for which the relative size of the parties concerned, the fact that a negotiation took place, or that certain provisions thereof might have been subject to such a negotiation and determined together by the relevant provider and business user is not, in itself, decisive». Therefore, it can be established that economic dimensions are considered indirectly and together with other circumstances of the overall assessment.

16 It can be noticed that Platform dimensions are also considered in the recent debate on the Digital Services Act. See European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)), 5, in which the European Parliament suggests the need for a framework manageable for small business, SMEs and start-ups.

purpose of concluding contracts with consumers[17].

In addressing these challenges, the regulation introduces three different levels of protection: the first concerns the terms and conditions of contracts; the second concerns contractual behaviour; and, finally, there is a specific discipline on alternative dispute resolution.

Levels of protection	Dispositions
1: T&Cs	• Article 3, §1 and §3; • article 5; • article 6; • article 7; • article 8, letters b) and c); • article 9; • article 10;
2: Contractual execution	• Article 3(2) and (4); • article 4; • article 8, letter a);
3: ADR	• Article 11; • Article 12; • Article 13;

2. Terms and conditions.

The Reg. (EU) n. 1150/2019 introduces, as first level of protection, a legal discipline for contracts between business users and providers of online intermediation services. It sets several requirements for contractual terms and conditions unilaterally determined by providers

Reg. (EU) n. 1150/2019 establishes, as a first level of protection, several requirements for contractual conditions unilaterally determined by providers of online intermediation services[18].

Art. 3(1), letters a) and b) refer to all terms and conditions and require a certain language to be used in their drafting and their accessibility for business users at all stages of contractual relations, including the pre-contractual stage. This general provision establishes a formal level of protection for business users and highlights the perspective adopted in the regulation. The vulnerable party, in his capacity as a trader, can adequately assess the convenience and meaning of the contract and for this reason it was considered sufficient to provide them with all the necessary information. Therefore, it was not considered necessary to introduce a

[17] For this reason, some of the usual services offered by online platforms are excluded from the scope of the Regulation, such as online payment services, online advertising tools or online advertising exchanges if they are not involved in concluding contract with consumers.
This limitation responds to the idea of a modular approach facing the presence of many different types of platform services. See J Campos Carvalho, 'Online Platforms' (n 1) 874. On the other hand, C Twigg-Flesner, 'The European proposal' (n 1) 226, highlights a certain concern about offers that target both consumers and business operators.

[18] This profile is the consequence of the prevision of art. 2, defining terms and conditions: « all terms and conditions or specifications, irrespective of their name or form, which govern the contractual relationship between the provider of online intermediation services and its business users and are unilaterally determined by the provider of online intermediation services, […]». The second part of the definition sets out the elements to be considered in assessing the unilateral determination, in order to clarify the extent of the burden of proof for business users. This choice has been criticised by C Twigg-Flesner, 'The European proposal' (n 1) 226, as an illustration of the difficulties that a coherentist approach creates in dealing with a new market model.

substantive limitation of the contract terms, as long as they are «drafted in plain and intelligible language».

The general requirements are complemented by provisions on specific terms and conditions. These provisions set out the mandatory content for each contract between commercial users and online intermediation service providers, requiring explicit indication for many contents, such as the reason for the providers' decision to limit, restrict or terminate the contract, any other distribution channel or programme offered, aspects relating to intellectual property rights[19], contractual conditions that must be based on good faith and fairness[20], and access to data generated on the platform[21]. Other necessary content relates to the ancillary goods and services provided by the platform itself or by third parties[22], and to the ADR systems provided for in articles 11 and 12, relating to the third level of protection.

Besides those contents, other provisions are related to the most problematic and discussed aspects of the new contractual relations.

First of all, art. 5 addresses the issue of ranking. The algorithms of the online platforms select and order the offers of commercial users according to specific criteria. This order determines the ranking of each individual offer. On the one hand, this system can guarantee a high level of fairness and transparency in the market as a corrective to information asymmetry, through the reputation of the platform[23]. Indeed, the order of offers could signal users' preferences or suppliers' trustworthiness and thus support responsible and consistent consumer choices. On the other hand, ranking can significantly influence the convenience of the service for business users and is closely linked to the functioning of the provider's algorithms. Therefore, the European institutions have tried to balance the interest of business users to fully understand the ranking mechanism and the need of providers to keep the essential aspects of their algorithm secret. The result is the requirement to disclose in the terms and conditions «the main parameters determining ranking» and the reasons for

---

[19] Art. 3(1) is supplemented by the obligation on providers to inform commercial users of these three terms. It is interesting to distinguish these terms from the others specifically considered, because only for their violation is nullity provided for.

[20] Article 8, entitled 'Specific contractual terms', prohibits retroactive changes to the terms and conditions, unless they are beneficial to business users or required by a legal or regulatory obligation. The provision also requires that the contract indicate the conditions under which business users may terminate their contractual relationship with the platform; and describe the treatment of information provided or generated by the business user after termination of the relationship. The content of this article can be considered as a combination of the first two levels of protection.

[21] This issue is divided into three different aspects: access for platforms to data provided by business users or consumers; access for business users to data generated by themselves or other operators or consumers in the use of the intermediation services; finally, access for third parties to these data. The first two aspects require to indicate which data are accessible and under what conditions; instead, data sharing with third parties requires the specification of its purpose and whether business users can opt out.
As clear, limitation for access to data is not considered, but it is only imposed to indicate among contractual terms the kind of data, the conditions of the access and its purpose.

[22] In particular, art. 6 requires among contractual terms a description of their type and the specification of possibility and conditions for the business user to offer its own ancillary goods and services.

[23] At the base of the issue G Akerlof, 'The Market for « Lemons »: Quality Uncertainty and the Market Mechanism' (1970) 84 The *QJEcon*, 488; A D Thierer, C Koopman, A Hobson and C Kuiper, 'How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the 'Lemons Problem'' (2016) 70 *U. Miami L. Rev.*, 830.
Furthermore, see A Wiewiorowska-Domagalska, *Online Platforms*, (n 1) 7; S Casabona, 'Intermediazione digitale' (n 7) 497; B de Langhe et al., 'Navigating by the Stars Investigating the Actual and Perceived Validity of Online User Ratings' (2015) 6 *J.Consum.*, 817 – 833; G Smorto, 'Reputazione, fiducia e mercati' (2016) 1 *Europa dir. priv.*, 199–218; G Giannone Codiglione, 'Reputazione online, sistemi di rating e anonimato in una recente decisione della corte di cassazione tedesca' (2015) 1 *Dir. Informatica*, 178–191; Idem, 'Algoritmi reputazionali e confini dell'autonomia dei privati' (2019) 2 *Dir. Informatica*, 520 – 540.

preferring them[24]. In addition, art. 5(6), clarifies that online intermediary service providers are not required to disclose algorithms, in accordance with Directive (EU) 2016/943.

This balancing can be considered adequate for the purpose of allowing business users to understand how to influence and improve their ranking, but it presents some critical issues concerning the actual possibility of understanding how the algorithm works, especially in relation to the number of criteria that can be involved[25]. Furthermore, it can be argued that art. 5, does not mention the dependence of the ranking of the offer on the feedbacks of consumers. This latter aspect is considered in other articles[26], but a clear indication in the terms of the contract would have been preferable. However, the European Commission supports the objective of a clear understanding of the ranking system through the development of guidelines on ranking transparency[27].

The Regulation also addresses the critical issue represented by the possibility for an online intermediation service provider to act as a supplier of goods and services by itself or through other controlled business users. At a first level, Ar. 7(1), requires that the terms and conditions describe the differential economic, commercial and legal treatment provided for offers directly or indirectly referable to the platform. Particular attention must be paid to access to data, ranking and other setting suppliers, remuneration charged for the intermediation or other functionalities or ancillary services.

This is one of the main concerns about online platforms; they often only mediate between suppliers and customers, but in a significant number of cases they act as market players rather than market makers. Consequently, there would be clear advantages that platforms can receive by offering goods and services, in terms of data, or better conditions of use of the platform that can lead to several competition problems with their users. However, the European institutions have chosen to prohibit a direct or indirect role of suppliers for platforms. The regulation, again, only requires that specific and clear information be included in the contractual conditions, so that business users can assess the convenience of the services.

A formal approach, finally, is adopted in relation to the so-called Most Favourite Nation (MFN) Clause.

In particular, art. 10 Reg. (EU) n. 1150/2019 regulates clauses that restrict the freedom of business users to offer the same goods and services under different conditions «through other means». If the platform decides to impose such a restriction, it is obliged to indicate this in contractual terms and conditions, specifying the «main economic, commercial and legal consideration» at the basis of the decision. Moreover, art. 10(2), clarifies that compliance with the formal obligation laid down in § 1 does not preclude any prohibition or limitation

---

[24] In particular, the possibility «to influence ranking against any direct or indirect remuneration», if included among parameters, have to be indicated.
Concerns for consumer protection are implied in ranking system related to remuneration. Therefore, art. 3(7), Dir. (EU) n. 2161/2019 inserts point 11a) to Annex I Dir. 2005/29/CE in order to list the conduct of platform consisting in «providing search results in response to a consumer's online search query without clearly disclosing any paid advertisement or payment specifically for achieving higher ranking of products within the search results» among commercial practice which are in all circumstance considered unfair.

[25] For concerns related to the high number of parameters considered see C Twigg-Flesner, 'The European proposal' (n 1) 227.

[26] Art. 5(4), Reg. (EU) 1150/2019 requires providers of online search engines to allow corporate website users to inspect the content of notification by third parties that caused a delisting. There isn't a similar provision in art 5 for providers of online intermediation services. The reason is that delisting can be considered as a case of restriction or suspension of the service, addressed in art. 4(5).

[27] See European Commission, 'Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council' (2020/C 424/01).

for those restrictions arising from the application of other Union or Member State law[28].

The issue of MFN clauses has taken on significant legal importance, both from a competition and a contractual point of view. Competition authorities have analysed the possibility of anti-competitive use of MFN clauses and many proceedings have allowed a restricted version of these clauses

The issue of MFN clauses has come up in the legal sphere, both from the competition and the contractual point of view. The Competition Authorities of several States have analysed the possibility of anti-competitive use of MFN clauses and many proceedings have allowed a restricted version of these clauses[29]. Other concerns relate to the significant limitation of the freedom to determine the content of business operators' offers resulting from the imposition of MSN clause. Therefore, in consideration of the relevance of the clause, the European institutions decided to take into account the issue.

Clearly, Reg. (EU) n. 1150/2019 does not introduce any limitation or prohibition for the MFN clause, providing for a transparency requirement in the terms and conditions, without any indication of the relevant sanction. At the same time, rules of member states that may even prohibit their use are expressly allowed. This approach cannot be considered adequate to the challenges of new contractual relationships, and contradicts the objective of achieving a uniform legal framework for digital platform contracts in Europe[30].

---

[28] It is interesting to consider that, in this case, the regulation itself show a certain awareness of the insufficient level of protection established.

An Example of legal prohibition can be found in Italian Law. See art. 1(166), l. n. 124/2017: «È nullo ogni patto con il quale l'impresa turistico-ricettiva si obbliga a non praticare alla clientela finale, con qualsiasi modalità e qualsiasi strumento, prezzi, termini e ogni altra condizione che siano migliorativi rispetto a quelli praticati dalla stessa impresa per il tramite di soggetti terzi, indipendentemente dalla legge regolatrice del contratto». Moreover, similar provisions have been introduced in France (art. 133 loi n. 2015-990 du 6 août 2015) and in Austria (law amending the Austrian Federal Act against Unfair Competition 1984, 16th July 2016). For the classification of the clause as a case of abuse of economic dependence see F Galli, 'La nullità della clausola MFN' (n 6) 1387.

[29] For the Competition relevance of these clauses see M Engels, T Brenner, A Rasek, 'Evaluating the abolishment of MFN clauses in the online hotel booking sector: the drawbacks of using price comparison data from meta-search sites' (2017) 11 *ECLR*, 483 – 490; M Colangelo, V Zeno-Zencovich, 'La intermediazione on-line' (n 1) 43.

In Europe MFN clauses have been analyzed by British OFT, documents of the proceeding are consultable at https://webarchive.nationalarchives.gov.uk/20140402153926/http://www.oft.gov.uk/OFTwork/competition-act-and-cartels/ca98/closure/online-booking/#named2 (accessed: 29th June 2020), by German Bundeskartellamt, Decision B9 121/13, consultable at www.bundeskartellamt.de (accessed: 29th June 2020), by Italian AGCM, Decision 21th April 2015, consultable at https://www.agcm.it/dotcmsDOC/allegati-news/I779_chiusura.pdf (last access: 30th June 2020); by French Autorité de la concurrence, Decision 21th April 2015, n° 15-D-06, consultable at https://www.autoritedelaconcurrence.fr/fr/decision/relative-des-pratiques-mises-en-oeuvre-dans-le-secteur-de-la-reservation-hoteliere-en (accessed: 29th June 2020); by Swedish Konkurrensverket, Decision, 15th April 2015, n. 596/2013, consultable at http://www.konkurrensverket.se/globalassets/english/news/13_596_bookingdotcom_eng.pdf (accessed: 29th June 2020). In particular, AGCM, Autorité de la concurrence and Konkurrensverket, accepted an identical proposal of commitment from Booking.com concerning a "Narrow MFN clause", i.e. restricted to direct offers from hotels, with the exception of discounts for "Closed User Group". Finally, the attention for price policies on Online Travel Agencies (OTAs) led to the realisation of a Report on the Monitoring Exercise Carried Out in the Online Hotel Booking Sector by EU Competition Authorities in 2016, consultable at https://ec.europa.eu/competition/ecn/hotel_monitoring_report_en.pdf (accessed: 29th June 2020).

Part of the doctrine pointed out a difference between MFN clause as defined in art. 10 Reg (EU) n. 1150/2019 and clauses imposed by OTAs. The first one provides a negative obligation, imposing not to concede better conditions in a contract with other agencies; the second allows the application of the best terms possibly provided through other means. See F Galli, 'La nullità della clausola MFN' (n 6) 1387; V Soyez, 'The compatibility of MFN clauses with EU competition law' (2015) 36 *ECLR*, 107.

[30] See F Galli, 'La nullità della clausola MFN' (n 6) 1387; C Twigg-Flesner, 'The European proposal' (n 1) 229.

A final criticism of the legal framework concerning terms and conditions is related to the contractual remedies for breach of the provisions. In fact, art. 3(3) defines as null and void only those contractual contents which violate the requirements of transparency and accessibility listed in arts 3(1) and 3(2).

On a first sight, the remedy is not appropriate for each infringement of art. 3(1). For instance, the absence of any indication of the ground for the right of termination of the contract cannot be remedied considering a non-introduced clause null and void. Thus, the sanction could relate to the act of termination adopted in the absence of the term authorising it, but cannot be suggested in case of general legal remedies for breach of contract[31].

On the contrary, there is not a specific remedy for violations of other articles. The choice not to introduce a general sanction of nullity is probably determined by the evidence that it is not applicable in every case. Indeed, some of the mandatory clauses introduced by the regulation do not confer rights on the parties, but only require clarification of aspects relevant to the evaluation of the convenience of the services. Therefore, the nullity of those contractual clauses cannot remedy the lack of knowledge which underlies those provisions. This circumstance is clear in arts. 5 and 7, which are even applicable in the absence of a contract, but the same is true for the indication of disparities for offers directly or indirectly proposed by the providers to customers or for the offer of ancillary good and services.

However, other cases would have suggested a different solution. In particular, inadequate provisions concerning access to data, or MFN clauses, would have been more efficiently remedied by treating the corresponding contractual term as null and void.

Finally, the information duties provided for in Articles 5, on ranking, and 7, on differential treatment, must also be respected, with the necessary variations, by online search engines in their relations with corporate website owners. In these cases, however, it is not possible to provide the information through contractual terms and conditions, so the Regulation requires them to provide «an easily and publicly available description» for the same aspects that are considered for providers of online intermediation services.

3. Rules for contractual relations.

The analysis of Reg. (EU) n. 1150/2019 suggests the existence of a second level of protection. It emerges from the provisions concerning those aspects of the contractual relationship between online intermediation service providers and business users that are not related to the content of the terms and conditions. These rules consider specific events that may take occur after the conclusion of the contract and impose specific obligations on platforms. Therefore, Regulation does not introduce this second stage of protection in relationships between providers of online search engines and corporate website owners, because of the absence of a contractual relation.

The European legislator has selected two relevant aspects as significant deviations from the ordinary performance of the contract: unilateral changes in contractual terms and conditions, in art. 3(2); and restriction, suspension or termination of contracts, in art. 4.

In addition to these two aspects, the provision of art. 3(5) can also be listed in the second level of protection, ensuring that the identity of the business user is clearly visible.

Art. 3(2) governs the manner in which an online intermediation services provider may unilaterally change terms and conditions. The provision requires several elements of protection: notification of changes on a durable medium; a period of notice to be observed before implementation of the changes, with a minimum duration of 15 days from the

[31] See C Twigg-Flesner, 'The European proposal' (n 1) 227.

notification[32]; the right of the business user to terminate the contract before expiry of the period of notice. This protection is supplemented by the prohibition of retroactive changes as set out in Art. 8.

However, the notice period may be waived if the business operator renounces, by written statement or clear affirmative action[33]; when changes are required to the provider by a legal or regulatory obligation in a way which does not allow it to comply with the notice period; or if the changes are necessary to address an unforeseen and imminent danger to the services[34].

The same protective purpose can be found in the rules governing the restriction, suspension or termination of contracts by providers. This is a sensitive aspect of the contractual relations under consideration, highlighting the great power of providers in the administration of their services.[35].

The first level of protection determines the necessary indication in the terms and conditions of the grounds for decisions to suspend or terminate or impose any other type of restriction on the intermediation services provided. Then, art. 4 establishes a second level of protection, requiring the manner in which this decision must be declared. This provision distinguishes between restriction and suspension of services, on the one hand, and termination, on the other. In both cases, the Regulation requires platforms to provide a statement of reasons for the decision on a durable medium to business users. This notification must contain certain information, listed in § 5. In particular, it must state the facts and circumstances of the decision, with particular regard to the contents of the third party notifications.

The last aspect indicated concerns the case in which one of these decisions is based on information notified by a third party to the online intermediation service provider. Such a situation may arise in the case of negative feedback from consumers, or notification of contractual violations by other business users. Negative feedback may lead to a restriction or suspension of services, especially in the form of a downgrade in the ranking of the offers[36].

In the case of other commercial users, an infringement notification may be justified by an interest in limiting competition on the platform and may represent a consistent criticality. The relevance of the concerns is compounded by the risk of abuse of the notifications that could lead to delisting[37]. These concerns have been brought to the attention of the

---

32 The notice period shall be longer if «this is necessary to allow business users to make technical or commercial adaptations to comply with the changes». see art. 3(2).

33 Such as submission of new goods and services to the provider during this period.

34 In particular, the norm considers «fraud, malware, spam, data breaches or other cybersecurity risks».

35 The right to suspend, limit or terminate contracts can be considered as a confirmation of the unbalanced bargaining power between providers of online intermediation service and their business users. The clause attributing a similar right is considered in art. 9(3), of Italian law n. 192/1998, as an exemplification of abuse of economic dependence, and consequently it can be considered null. See F De Leo, 'Sospensione dell'account da parte di Ebay: tecniche di risoluzione, clausole vessatorie e abuso di dipendenza economica' (2013) 6 *Resp. civ. prev.*, 2031; I P Cimino, 'Sospensione ingiustificata dell'account di vendita ed inadempimento di eBay' (2011) 4 *Contratti*, 351; E Bacciardi, 'Contratti telematici' (n 6) 381–391.

36 See 22th whereas: «short of being suspended, providers of online intermediation services can also restrict individual listings of business users; for example, through their demotion or by negatively affecting a business user's appearance ('dimming') which can include lowering its ranking».
In this sense Consumer evaluation could become a sanction for business users. See V Zeno-Zencovich, 'Comunicazione, reputazione, sanzione' (2017) 2 *Dir. Informatica*, 263-275; G Smorto, 'Reputazione' (n 22) 199-218.

37 The Regulation considers this issue even in case of providers of online search engine in 26th whereas, but it is required only a publicly accessible online database, due to the absence of a contractual relationship. This measure can allow corporate website user to inspect the contents of the notification, helping them to mitigate potential abuses, by competitors, of notifications that could lead to delisting.

Competition Authorities[38].

Despite the importance of the issue, the Regulation only requires the content of these notifications to be communicated to the operators to whom they relate, without any adequate system for verifying them. This choice placed the burden of defence on commercial users. In fact, the regulation provides for the possibility for them to clarify the facts and circumstances that justified the provider's decision, through the internal compliant-handling process (art. 11) [39].

Moreover, the statement of reasons is not always required. In fact, art. 4(5) allows this duty to be waived in the event a legal or regulatory obligation not to provide reasons, or in case of repeated infringements of term or condition by users.

The required noticed period varies: the decision to restrict or suspend the service may even be communicated at the time when it applies; in the case of termination, art. 4(2) imposes that notice must be given at least 30 days before the decision takes effect. Again, the notice period may be avoided for different reasons; the first one is the same for changes in terms and conditions; the second refers to to compelling reasons under national and Union law, and may include the reason indicated in Art. 3(5)(b); finally, a third case is introduced referring to repeated infringements of terms and conditions.

In conclusion, the Regulation employs an essentially formal approach also for the level of protection analysed above. Duties of information were preferred to the imposition of a limitation of the power to change the terms or to restrict or terminate the contract. It can be argued that the European institutions have adopted the concept of procedural good faith in determining this legal framework, requiring only that a procedure inspired by a legal assessment of good faith and fairness be followed. This procedure finally lead only to the choice for business users to terminate the contract, in case of contractual changes, or to defend themselves in the internal compliant-handling process, in case of restriction, suspension and termination.

4. Alternative dispute resolution.

The third level of protection developed for commercial users of online platforms consists of alternative dispute resolution (ADR) and law enforcement requirements. It can be considered as the closure of the protection system. The fundamental role of this level of protection responds to the need for business users to easily and conveniently raise their complaints about both technical and legal issues arising in the performance of the contract[40].

The required ADR comprises two different models: an internal compliant-handling system, disciplined in art. 11; and the indication of mediators, imposed by art. 12. The relevance of those requirements is highlighted by their necessary indication in terms and

---

[38] See on the point AGCM, 19th December 2014, consultable at https://www.agcm.it/dotcmsDOC/allegati-news/PS9345_scorrsanz_omi.pdf (accessed: 29th June 2020), in which Italian AGCM condemned Tripadvisor for an unfair commercial practice (arts. 18 ff cod. cons.) consisting in claims concerning the genuine content of its reviews. The decision was then annulled with the sentence Tar Roma, (Lazio) sez. I, 13th July 2015, n. 9355, (2015) 3 *Dir. Informatica*, 494; but, finally, it has been confirmed by Cons. St., sez. VI, 15th July 2019, n. 4976, (2020) 4 *Foro it.*, 246.
See L Vizzoni, 'Recensioni non genuine su Tripadvisor: quali responsabilità?' (2018) 2 *Resp. civ. prev.*, 706-722; L Carota, 'Diffusione di informazioni in rete e affidamento sulla reputazione digitale dell'impresa' (2017) 4 *Giur. Comm.*, 624-638; A De Franceschi, 'The Adequacy of Italian Law for the Platform Economy' (2016) 5 *EuCML*, 56.

[39] A favorable conclusion of this process shall determine the reinstate of the users without delay.

[40] Many online platforms, such as Booking, Airbnb, Paypal, Amazon and eBay, provide a system of resolution concerning dispute between suppliers and customers. On this topic see S Casabona, 'Intermediazione digitale' (n 7) 497. The Regulation does not require the implementation of these systems, having regard only for dispute between business users and providers of online intermediation services.

condition

The required ADR comprises two different models: an internal complaint-handling system, regulated in art. 11; and the indication of mediators, required by art. 12. The relevance of these requirements is highlighted by their mandatory indication in the terms and conditions of the contract[41].

However, the system has an important limitation: both of these articles do not apply to providers of online intermediation services that are small enterprises in the sense clarified in the Annex to Recommendation 2003/361/EC.

The internal complaint-handling system ensures a rapid and inexpensive resolution of disputes arising in the regulated contractual relationships. As Art. 12(1), requires, it «shall be easily accessible», «free of charge for business users» and reasonably expeditious. The Regulation also lists the essential principles of the system, which are transparency, equal treatment and proportionality to the importance and complexity of the complaint. In addition, Art. 11(2), prescribes general arrangements for the process, and Art. 12(4), requires readily available information on its function and effectiveness.

The most important aspect of the Framework is the list of issues to be considered in the system. They are, according to art. 11(1)(2): (a) the failure of providers to comply with any of the obligations of the regulation, (b) technological issues that directly affect the provision of online intermediation services, and (c) measures taken by, or the conduct of, providers directly related to the services.

Subparagraphs (a) and (b) concern technical and legal issues relating to the provision of online intermediation services. In particular, sub-paragraph (a) requires an effective and rapid resolution of all complaints relating to the application of the Regulation. Consequently, it is possible to consider the complaints management system as a first and private level of enforcement of the legal framework.

In addition, subparagraph (c) extends the relevant issues to those relating to decisions of the platforms which may affect the convenience of the services for business users. In this sense, the compliant-handling system can be involved in the realisation of the right to clarification of the facts and circumstances that led to the platform's decision to limit, suspend or terminate the contract, as set out in Art. 4(3).

The regulation also obliges platforms to provide for a mediation system. In particular, art. 12(1) requires platforms to identify two or more mediators[42] in the terms and conditions of the contract in order to make business users aware of their right to settle the dispute out of court. In order to ensure the effectiveness of the system, the regulation requires that the costs of mediation be reasonably borne by both parties. In particular, this proportion is to be established by the mediator, according to several criteria exemplified in art. 12(4)[43].

Mediation does not impede a recourse to judiciary proceedings, as it remains essentially

---

41 Art. 11(3), establishes that platforms have to provide «all relevant information relating to the access to and functioning of their internal complaint-handling system»; and art. 11(1), oblige providers to identify in their terms and conditions two or more mediators.

42 The Regulation requires the Commission and Member States to encourage providers of online intermediation services to set up organizations providing mediation, with the purpose of facilitating the out-of-court settlement. See art. 13. The regulation describes all requirements that mediators shall meet, in art. 12, §2, such as, impartiality and independence, affordable costs for business users, language of the mediations, easy physical or remote access, mediation without delay and sufficient understanding of general business-to-business relations. It is also possible to identify mediators outside Europe if they ensure the application of benefits deriving from Union and Member State law.

43 They are: «the relative merits of the claims of the parties to the dispute, the conduct of the parties, as well as the size and financial strength of the parties relative to one another». See art. 12(4).

voluntary for parties[44]. However, the need for ADR to be effective means that business users and providers of online intermediation services must engage in good faith this procedure[45].

Finally, art. 14 allows representative organisations or associations of business users or public bodies of Member State to stop or prohibit any non-compliance with relevant requirements of the Regulation. This provision ensures that infringements of the Regulation can be repressed if «various factors» would «obstacle the business users recourse to the judge»[46].

Conclusions.

The brief analysis of the principal aspects of Regulation (EU) n. 1150/2019 makes clear the fragile balance achieved between the interests of the professional parties involved in the online platform market. The European legislator has adopted a contractual and formal approach, consisting of three levels of protection that are not fully adapted to the protection needs of business users[47], especially if compared to the consumer protection *acquis*. This formal approach does not solve several issues related to platform contracts.

First of all, the articles on terms and conditions do not impose any substantive limitations on the rights and obligations of the parties. Thus, the legal framework allows online intermediary service providers to introduce any contractual clause, even a significantly unbalanced one, as long as it is clearly and intelligibly stated in the contractual contents. Even if this formal protection could be seen as responding to the characteristic distinction between the vulnerabilities of commercial users and those of consumers, the regulation should have been more stringent in determining the legal framework relating to ranking, the MFN clause and the right to suspend, restrict or terminate contracts unilaterally. Indeed, these clauses can impose a significant limitation on the contractual freedom of the parties.

As a second level of protection, the regulation requires procedural good faith for the most significant events in the performance of the contract. The legal framework may be considered adequate for the purpose of legal protection of business users in the event of unilateral changes to the content of the contract, but there are still concerns about the most controversial aspect in the contractual relationships considered. In particular, for the legal protection against restriction, limitation or termination of the contract imposed on business users by platforms, there is no adequate protection. In particular, the regulation ignores the problem of verifying the reliability of notifications or negative feedback from third parties.

Finally, the third level of protection, introducing two degrees of ADR, i.e. complaint and mediation, can be considered adequate to the objective of avoiding the expensiveness and length of court proceedings. However, its practical relevance could be affected by uncertainties in the rights of the parties. In particular, the lack of substantive protection in terms and conditions, and the uncertainty of the remedies granted to business users in the event of a violation of the regulation may impede effective protection even through recourse to ADR.

---

[44] Art. 12(5), Reg. (EU) n. 1150/2019.

[45] Art. 12(3), Reg. (EU) n. 1150/2019.

[46] See 44th whereas Reg. (EU) n. 1150/2019: «Various factors, such as limited financial means, a fear of retaliation and exclusive choice of law and forum provisions in terms and conditions, can limit the effectiveness of existing judicial redress possibilities, particularly those which require business users or corporate website users to act individually and identifiably. To ensure the effective application of this Regulation, organisations, associations representing business users or corporate website users, as well as certain public bodies set up in Member States, should be granted the possibility to take action before national courts in accordance with national law, including national procedural requirements».

[47] See C Twigg-Flesner, 'The European proposal' (n 1) 232, who considered the proposal of the Regulation to be too timid.

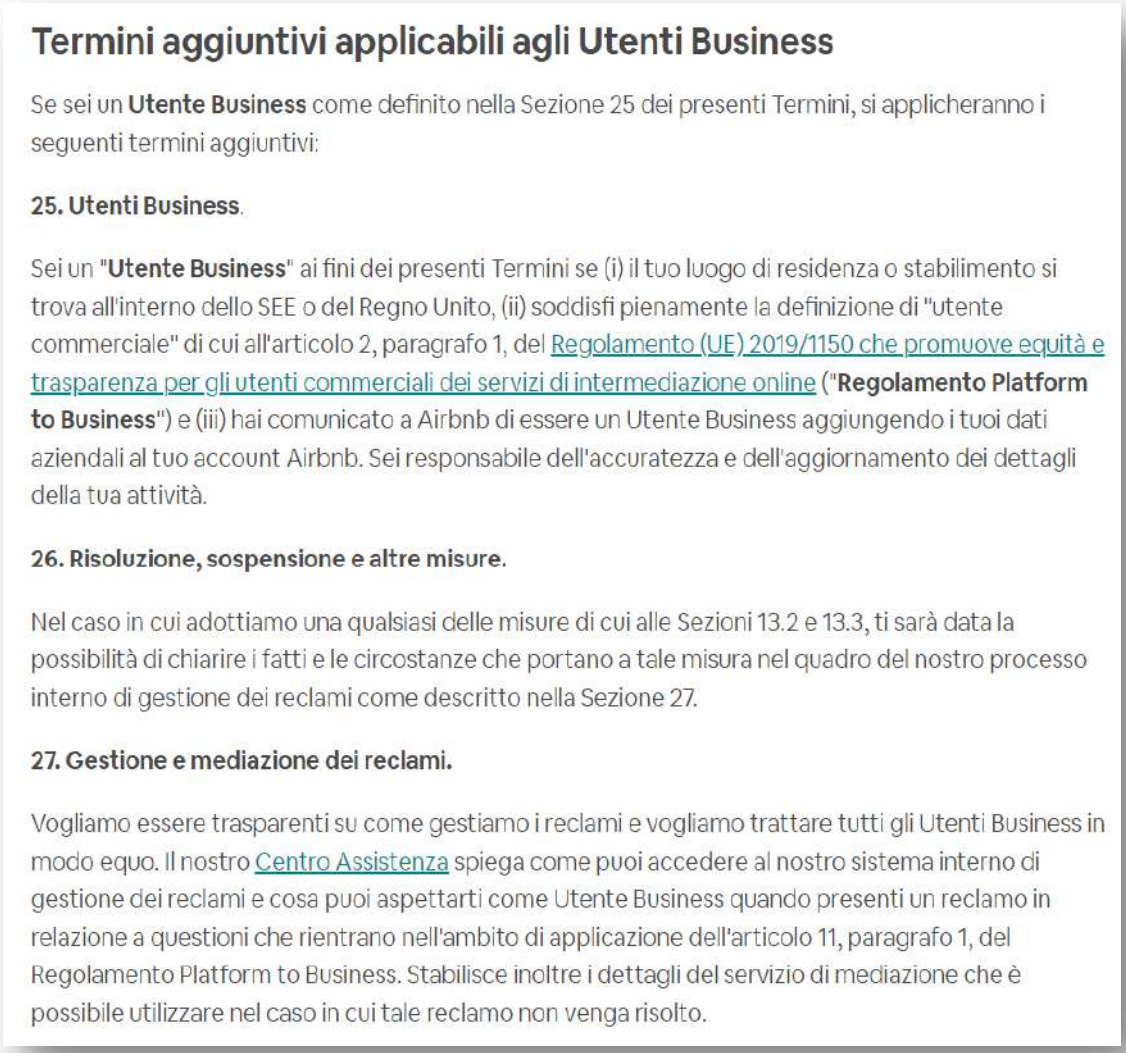
The critical issues highlighted and the choice of the contractual perspective[48] without clear harmonisation rules may lead to the failure of the aim of ensuring legal certainty through a single regulatory framework in Europe. It can be argued that the domestic law of the Member States will be invested in completing the protection granted to business users.

For instance, from an Italian perspective, the most controversial aspects of the contractual relationship should be addressed through the application of general requirements for the right to terminate the contract, with particular regard to clauses considering non-performance. In this sense, an adequate description of each relevant non-performance as in art. 1456 of the Italian Civil Code, or alternatively a requirement of seriousness for breaches as in art. 1455, may be required in addition to the provisions of the regulation.

Finally, a clear level of protection can be afforded by applying art. 9 l. n. 192/1998 on the abuse of economic dependence. This particular situation can occur in the relationship between online platforms and commercial users, especially in cases where the latter offer a relevant part of their product or service through the platform. In addition, many of the aspects of these contracts lead to hypotheses of abuse, such as the MFN clause and the provisions introducing arbitrary bases of suspension, termination or limitation of the service. Therefore, the application of art. 9 can lead to the remedy of nullity for the most problematic aspects considered in the regulation, completing the level of protection established.

In conclusion, the analysis of Reg. (EU) n. 1150/2019 shows an ambiguous approach of the European intervention. On the one hand, it responds to the need of legal protection for business users of online intermediation services; on the other, the protection model adopted reveals a scrupulous consideration of the interest of platforms, in order not to freeze the development of the so-called collaborative economy. In other words, it can be said that the European institutions, in determining the necessary level of protection, were more concerned with the widespread use of platforms than with the vulnerability of commercial users. Even if a full consideration of legal remedies at the domestic level may resolve some problematic aspects of the Regulation, it can be concluded that the intervention of the Regulation is largely disappointing in the perspective of a more comprehensive and uniform legal framework.

[48] Some scholars have suggested a different legal intervention in view of the coordination that a contractual approach would require. This issue is particularly evident in relation to national contract law or the European consumer acquis. See C Busch, H Schulte-Nölke, A Wiewiorowska-Domagalska, F Zoll, 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law?' (2016) 5 *EuCML*, 3–10; T Rodriguez de las Heras Ballell, 'The Legal Anatomy of Electronic Platforms: A prior study to assess the need of a Law of Platforms in the EU' (2017) 1 *ItaLJ*, 149-176; C Twigg-Flesner, 'The European proposal' (n 1) 231.



Termini aggiuntivi applicabili agli Utenti Business

Se sei un **Utente Business** come definito nella Sezione 25 dei presenti Termini, si applicheranno i seguenti termini aggiuntivi:

25. Utenti Business.

Sei un "**Utente Business**" ai fini dei presenti Termini se (i) il tuo luogo di residenza o stabilimento si trova all'interno dello SEE o del Regno Unito, (ii) soddisfi pienamente la definizione di "utente commerciale" di cui all'articolo 2, paragrafo 1, del Regolamento (UE) 2019/1150 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online ("**Regolamento Platform to Business**") e (iii) hai comunicato a Airbnb di essere un Utente Business aggiungendo i tuoi dati aziendali al tuo account Airbnb. Sei responsabile dell'accuratezza e dell'aggiornamento dei dettagli della tua attività.

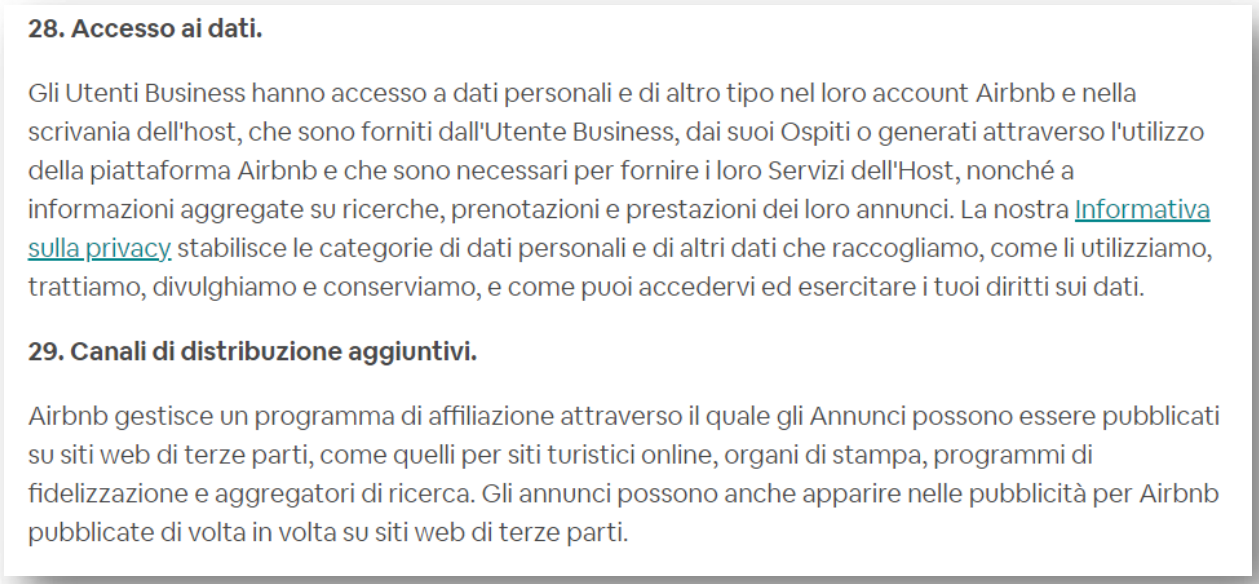
26. Risoluzione, sospensione e altre misure.

Nel caso in cui adottiamo una qualsiasi delle misure di cui alle Sezioni 13.2 e 13.3, ti sarà data la possibilità di chiarire i fatti e le circostanze che portano a tale misura nel quadro del nostro processo interno di gestione dei reclami come descritto nella Sezione 27.

27. Gestione e mediazione dei reclami.

Vogliamo essere trasparenti su come gestiamo i reclami e vogliamo trattare tutti gli Utenti Business in modo equo. Il nostro Centro Assistenza spiega come puoi accedere al nostro sistema interno di gestione dei reclami e cosa puoi aspettarti come Utente Business quando presenti un reclamo in relazione a questioni che rientrano nell'ambito di applicazione dell'articolo 11, paragrafo 1, del Regolamento Platform to Business. Stabilisce inoltre i dettagli del servizio di mediazione che è possibile utilizzare nel caso in cui tale reclamo non venga risolto.

An example: Terms and condition elaborated by Airbnb



28. Accesso ai dati.

Gli Utenti Business hanno accesso a dati personali e di altro tipo nel loro account Airbnb e nella scrivania dell'host, che sono forniti dall'Utente Business, dai suoi Ospiti o generati attraverso l'utilizzo della piattaforma Airbnb e che sono necessari per fornire i loro Servizi dell'Host, nonché a informazioni aggregate su ricerche, prenotazioni e prestazioni dei loro annunci. La nostra Informativa sulla privacy stabilisce le categorie di dati personali e di altri dati che raccogliamo, come li utilizziamo, trattiamo, divulghiamo e conserviamo, e come puoi accedervi ed esercitare i tuoi diritti sui dati.

29. Canali di distribuzione aggiuntivi.

Airbnb gestisce un programma di affiliazione attraverso il quale gli Annunci possono essere pubblicati su siti web di terze parti, come quelli per siti turistici online, organi di stampa, programmi di fidelizzazione e aggregatori di ricerca. Gli annunci possono anche apparire nelle pubblicità per Airbnb pubblicate di volta in volta su siti web di terze parti.

An example: Terms and condition elaborated by Airbnb

EJPLT

Online platforms: new vulnerabilities to be addressed in the European legal framework. Platform to consumer relations.

ROBERTA MONTINARO
Associate Professor at the University L'Orientale of Naples

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Abstract

The essay analyses the relationship between online platforms and consumers in the light of European consumer law. The complex digital environment shaped by platforms is characterised by a lack of transparency about the role and status of the parties active in the online marketplace, as well as by the use by online platforms of practices aimed at conditioning consumers' behaviour and limiting or completely excluding their self-determination, giving rise to new forms of vulnerability. In such a context, the regulation of unfair commercial practices can play a central role, provided that some interpretative uncertainties are overcome.

Keywords: online platforms - B2C contracts - unfair commercial practices - online advertising; differential pricing - vulnerable consumer.

Summary: Introduction. – 1. Rules on online marketplaces set forth by the modernization directive. – 2. Unfair commercial practices in platform to consumer relations. – 2.1. Practices amounting to forms of covert advertising: the uncertain boundary between information and advertising. – 2.2. Practices related to online ranking of goods and services. Personalized ranking. 2.3. Practices amounting to differential treatment in platform to consumers relations: price differentiation – 2.4. Personalization of advertising and targeting techniques in platform to consumer relations. – 3. Role played by UCPD rules in tackling the new forms of vulnerabilities arising in the context of platform to consumer dealings.

Introduction.

The European Commission, in its 2016 Communication on Online Platforms and the Digital Single Market - Opportunities and Challenges for Europe ('Platform Communication') highlighted the challenges that online platforms pose to consumer law[1] and called for the promotion of greater transparency when traders deal with consumers using such platforms, in particular with regard to goods/services' rankings and data collection. More recently, in view of these challenges, the Proposal for a Regulation on a Single Market For Digital Services (15.12.2020 COM(2020) 825 final; hereinafter DSA Proposal) recognized the need to amend and update first of all Directive 2000/31/EC[2] (hereinafter the E-Commerce Directive), but also other consumer law provisions applicable to online

[1] C. Busch, H. Schulte-Nölke, A. Wiewiórowska-Domagalska, F. Zoll, *The Rise of the Platform Economy: A New Challenge for EU Consumer Law?* (2016) 1 *EuCML*, 3.

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.

transactions between traders and consumers.

1. Rules on online marketplaces set forth by the modernization directive

A step in the direction suggested by the European institutions is represented by directive 2019/2161/UE (hereinafter "modernization directive"[3]) that has been adopted in order to (at least partially) adapt the provisions contained in the Unfair Commercial Practices Directive[4] (hereinafter "UCPD") and Consumers Rights Directive[5] (hereinafter "CRD") to the developments occurred in the digital economy, with the aim of strengthening consumers' rights when the latter engage in online transactions[6].

According to the modernization directive, online marketplaces consist of "a service using a software, including a website, part of a website or an application, operated by or on behalf of a trader which *allows* consumers to conclude distance contracts with other traders or consumers". This broad definition stresses the fact that online marketplaces fulfill an intermediation role bringing together and facilitating transactions between consumers and suppliers of goods and services; and that characteristic entails the presence of contractual relations that involve multiple parties playing different roles and having various legal status. The same definition takes into account that digital platforms are home to the active consumer (or prosumer[7]), so called because he or she has an active role in promoting products and services and enters into contracts with other consumers[8].

Given the complexity of the environment where digital platforms operate, it may not always be clear to the consumer who the parties to the supply contract are and what legal status the supplier of goods or services may have[9]. This opacity creates uncertainty about the

---

[3] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

[4] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L149/22.

[5] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance [2011] OJ L304/64, as amended by Directive 2015/2302/EU of the European Parliament and of the Council of 25 November 2015.

[6] The modernization directive has amended Directive 2005/29/CE, by adding a definition (article 2(lett. *n)* of "'online marketplace'. A similar definition has been included in the CRD (see Art. 2, 1 no. 16 and 18).

[7] M. Maugeri, *Elementi di criticità nell'equiparazione, da parte dell'AEEGSI, dei "prosumer" ai "consumatori" e ai "clienti finali"* (2015) *Nuova giur. civ. comm.*, 406. See also F. Trubiani, *I soggetti del commercio elettronico: limiti delle attuali definizioni legislative e prospettive future* (2020) 2, *Nuovo dir. civ.*,..

[8] D. Di Sabato, *Progredire tornando all'antico: gli scambi della sharing economy*, in *Sharing economy. Profili giuridici* (eds.) D. Di Sabato, A. Lepore (ESI 2018), 5.

[9] A. Quarta, *Il diritto dei consumatori ai tempi della* peer economy. *Prestatori di servizi e* prosumers, (2017) 2 *Europa e Diritto Privato*, 667. G. Smorto, *La tutela del contraente debole nella* platform economy (2018) *Giornale dir. lav. relaz. industriali*, 423.

legal framework applicable to the supply contract[10]. Therefore, when buying from an online marketplace, consumers need to be clearly informed about: i) the identity of the goods/services provider; ii) whether the online platform provider bears some of the duties arising from the supply contract; iii) whether they are buying goods or services from a trader or from a non-trader.

In this respect, CRD, as amended by the modernization directive, currently includes a new provision (art. 6 bis) that prescribes a series of transparency duties upon the providers of online marketplaces regarding, first of all, the legal status of the third party offering goods or services to consumers through the online marketplace and, secondly, whether the online marketplace acts as a mere intermediary between the parties to the supply contract.

Notably, under this provision, before a consumer is bound by a distance contract on an online marketplace, the provider of the online marketplace shall: *i)* inform consumers whether the third party offering goods, services or digital content is a trader or a non-trader, based on a declaration made by the same third party; *ii)* in case the third party is a non-trader, provide a short statement that consumer law does not apply to the contract concluded. The rationale of this provision resides in ensuring that consumers do not rely on the fact that their counterparty is a trader[11]. In light of the above, the modernization directive has added also a new art. 7, f), to the UCPD, according to which it is material the information "whether the third party offering the products on the online market place is a trader or not, on the basis of the declaration of that third party to the provider of the online marketplace ". Not providing this information amounts to an unfair practice and can be sanctioned as such.

Moreover, under the modernization directive, it is mandatory to disclose how the obligations related to the supply contract are shared between the third party offering the goods, services or digital content and the provider of the online marketplace. Consequently, the role of mere intermediary between the supplier of the goods or services and the consumer may be invoked by an online platform only if that role is made apparent by clear and comprehensible communication to consumers[12] (not entrusted to standard forms or the like). This principle, set out in various provisions of consumer law, is at the basis of previous case law according to which a trader acting (offline) as an intermediary on behalf of a private individual qualifies as seller for the purposes of Article 1(2)(c) of Directive 1999/44/EC[13],

---

[10] C. Twigg-Flesner, *Disruptive Technology – Disrupted Law? How the Digital Revolution affects (Contract) Law,* A. De Franceschi (ed.), *European Contract Law and the Digital Single Market*, 2016, 34-6.

[11] According to *European Commission, Staff Working Document on Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices*, SWD(2016)163 final, "under the professional diligence and transparency requirements laid down by Articles 5(2), 2(h), 6 and 7 UCPD, any e- commerce platform, insofar as it can be considered a "trader", should take appropriate measures enabling, amongst others, its users to clearly understand who their contracting party is – and the fact that they will only benefit from protection under EU consumer and marketing laws in their relations with those suppliers who are traders".

[12] See Recital n. 27 of the modernization directive: (for example, it could indicate that a third-party trader is solely responsible for ensuring consumer rights, or describe its own specific responsibilities where that provider assumes responsibility for certain aspects of the contract, for example, delivery or the exercise of the right of withdrawal).

[13] Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees [1999] OJ L171/12.

where the former has failed to duly inform the consumer of its role of mere intermediary[14].

In the same vein, building upon other existing case law[15], the modernization directive states that the information given by the provider of an online marketplace is without prejudice to any responsibility that the latter and the third-party trader have in relation to the supply contract under other Union or national law. This means that the determination of the duties incumbent on the online marketplace provider as a result of the supply contract is a matter of interpretation that must be assessed on a case-by-case basis.

2. Unfair commercial practices in platform to consumer relations

Online marketplace providers often resort to forms of commercial practices, which are able to influence consumers' preferences and needs and oftentimes to compromise their self-determination and freedom to choose goods and services[16]. Such practices are made possible by the deployment of digital technologies and involve the collection[17], use and transfer of consumer data to third parties and therefore affect both consumer law and data protection law[18].

2.1. Practices amounting to forms of covert advertising: the uncertain boundary between information and advertising.

Among the practices that can threaten consumer autonomy are forms of covert advertising, which frequently occur on online platforms. These practices are made possible by the fact that - in the context of online interactions between traders and consumers - the boundaries between genuine information (or recommendation) and advertising have become blurred. Digital platforms tend to take advantage of this opacity.

---

[14] European Court of Justice, Judgment of the Court (Fifth Chamber) of 9 November 2016, *Sabrina Wathelet v Garage Bietheres & Fils SPRL* (Case C-149/15).

[15] See CGUE *Uber Spain* (C-434/15), 20th December 2016; *Uber France* (C-320/16), 10th April 2018; *AirBnB Ireland* (C-390/18), 19th December 2019. A. De Franceschi, *Uber Spain and the identity crisis of online platforms*, (2018) *Journal of European Consumer and Market Law*, 1.

[16] Wolfie Christl, *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* (2017); P. Nguyen, L. Solomon, *Consumer data and the digital economy: Emerging issues in data collection, use and sharing* (2018) 1-62, 11, available at https://apo.org.au/sites/default/files/resource-files/2018-07/apo-nid241516.pdf. Online platforms tend to make use of consumers' data in order to influence their economic self-determination. See in this respect E. Mik, *The erosion of autonomy in online consumer transactions*, (2016) 8(1), *Law, Innovation and Technology*, 1-38.

[17] A. Jablonowska, M. Kuziemski, A.M. Novak, H.W. Micklitz, P. Palka, G. Sartor, *Consumer Law and Artificial Intelligence. Challenges to the EU Consumer Law and Policy Stemming from Business' Use of Artificial Intelligence* (Final report of the ARTSY project), (2018) *EUI Working Papers*, 35: "Data gathering and knowledge generation might be the most fundamental "use" of AI by business… It was the availability of big data – the "dataquake" – that enabled high-paced development and mass deployment of AI in the first place; data not necessarily actively collected, but also generated as a side product of consumer use of online platforms and services".

[18] These practices are mostly made possible by the ability of platforms to analyze and relate huge amounts of data, as well as the use of Artificial Intelligence systems. See on these aspects N. Helberger, B.F. Zuiderveen, A. Reyna, *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law* (2017) 54 *Common Market Law Review*, 1427 and G. Sartor, *New aspects and challenges in consumer protection. Digital services and artificial intelligence*, April 2020, 24, available at *https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648790/IPOL_STU(2020)648790_EN.pdf*

One example of these kinds of practices is the endorsement[19], recurring on social media platforms, of goods and services by the so-called influencers, who present themselves as mere disinterested users, but in fact recommend products/services on behalf of a supplier; this form of communication (being part of an entertainment content created by users of the digital platform) has a pronounced persuasive effect on the recipients of this form of communication (especially on minors[20]), that can be difficult to neutralise[21].

The circumstance, therefore, of not clearly stating that it is a communication with a commercial intent makes the practice unfair under the UCPD's provisions, according to which any form of commercial communication must be clearly identifiable as such by the recipients of the communication[22]. In this regard, however, an important question is identifying the party that should reasonably be expected to perform these duties (between the supplier and the influencer) and whether the platforms have to meet also any transparency obligations. Those issues have been the subject matter of Market Authorities' decisions[23].

A similar practice in terms of persuasiveness and opacity is represented by the review/rating of goods or services offered to consumers within an online marketplace by other consumers that claim to have experienced them. This type of review is enabled by the provider of the online marketplace that makes available to its users and manages a system of reputational feedback[24]. This practice has the merit of allowing consumers to easily obtain information from sources other than the companies themselves that provide the reviewed products/services. However, it can be used in a way that distorts the economic behavior of consumers and in light of this, first of all, businesses are required by the modernization directive to ensure that such practices are transparent and truthful[25]; moreover, Annex 1 to

---

[19] Commercial users of these platforms incorporate product advertising into their entertainment content and give the impression that the content is not advertising in the first place. See S. C. Boerman, N.Helberger, G. van Noort, C. J. Hoofnagle, *Sponsored Blog Content: What Do the Regulations Say: And What Do Bloggers Say* (2018) 9(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 146 ; C. Riefa, L. Clausen, *Towards fairness in Digital Influencers' Marketing Practices* (2019) 8 Journal of European Consumer and Market Law, 64.

[20] Younger users are often unable to distinguish independent recommendations from product placement. See I. GARACI, *La "capacità digitale" del minore nella società dell'informazione*, (2019) *Nuovo dir. civ*., 59, 79.

[21] R. Baldwin, *From Regulation to Behavior Change: Giving Nudge the Third Degree*, (2014) 77(6) *Modern Law Review*, 831.

[22] See Article 7(2) and point No. 22 of Annex I UCPD against hidden marketing. A similar requirement stems from Article 6(a) of the e-Commerce Directive.

[23] See the Italian Autorità Garante della Concorrenza e del Mercato (AGCM), Order no. 27787 of the 22.5.2019 https://www.agcm.it/dotcmsCustom/tc/2024/6/getDominoAttach?urlStr=192.168.14.10:8080/C12560D000291394/ 0/E6B624BBD0F6A573C12584150049D1EE/$File/p27787.pdf).

[24] C. Busch et al., *The ELI Model Rules on Online Platforms*, in *European Consumer and Market Law*, 9, 2, 2020, 61 ss.; C. Busch, *Crowdsourcing Consumer Confidence: How to Regulate Online Rating and Review Systems in the Collaborative Economy*, (ed.) A. De Franceschi, *European Contract Law and the Digital Single Market*, (2016) Cambridge, 223; G. Smorto, *Reputazione, fiducia e mercati* (2016) 1 *Europa e diritto privato*, 199; A. Thierer, *How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the "Lemons Problem"* (2016) 70 *University of Miami Law Review*, 830.

[25] J. Malbon, *Taking Fake Online Consumer Reviews Seriously*, (2013) 36 *Journal of Consumer Policy*, 139. See also Competition and Markets Authority (UK), *Online reviews and endorsements – Report on the CMA's call for information*,

Dir. 2005/29/EC has been amended so as to include among the list of unfair commercial practices also those consisting in "Sending, or instructing another legal or natural person to send, false consumer reviews or false appreciations or providing false information about consumer reviews or appreciations on social media, in order to promote products" (Art. 23 ter), as well as in "Indicating that reviews of a product are sent by consumers who have actually used or purchased the product without taking reasonable and proportionate measures to verify that the reviews come from such consumers" (Art. 23 bis) [26].

2.2. Practices related to online ranking of goods and services. Personalized ranking.

Practices related to the classification of the results of online searches for goods and services conducted by consumers in digital marketplaces are also expressly regulated by the modernization directive. Indeed, it is well known that higher ranking or any prominent placement of commercial offers within online search results has an important impact on consumers' choices. There are a range of factors which might influence the order in which search results are presented and each online platform has its own algorithm which determines the order of presentation.

In light of that, in order to promote transparency, the modernization directive clarifies that, although it is permissible for a business user to pay an online market, whether directly or indirectly, to "influence rankings", nevertheless, this fact must be disclosed, along with the effect of such payment on the ranking. Consequently a new item has been added to Annex I of Directive 2005/29/EC, to make it clear that practices where a trader provides information to a consumer in the form of search results in response to the consumer's online search query, without disclosing paid advertising or payment made specifically for achieving higher ranking of products within the search results, are unfair and sanctioned as such. This is a transparency requirement designed primarily to protect the freedom of choice of the consumer who may be unaware that the results of the online search are influenced by third parties or the economic interests of the online marketplace provider. Such a transparency requirement applies also to comparison tools[27].

At the same time, it is expressly mandated that platforms set out the "main parameters determining ranking"[28], as well as the relative importance between the various parameters, and provide this information in a clear and comprehensible manner, not being sufficient to this end a mere "reference in the standard Terms or Conditions"(Recital 19). In this respect, the EU Commission had already clarified that consumers, unless are informed otherwise, have the expectation that search results are included and ranked based only on relevance to their search queries and not based on other criteria (p. 133).

The new rules implicitly recognize that, besides the issue of influence exerted on behalf

---

CMA41 (June 2015) and ISO 20488:2018, *Online consumer reviews – Principles and requirements for their collection, moderation and publication*.

[26] See Recitals no. 47 and 49.

[27] The UCPD requires all traders to clearly distinguish a natural search result from advertising. This also applies to operators of comparison tools. The relevant provisions in this respect are Article 6(1)(c) and (f) and Article 7(2) UCPD. See in this respect the 'Key principles for comparison tools', http://ec.europa.eu/consumers/consumer_rights/unfair-trade/comparison-tools.

[28] It is not mandated to make public the algorithm that determines the ranking, in view of the need for reconciling the transparency about the way rankings work with protection of trade secrets and intellectual property.

of third parties, the way algorithms that determine the rankings of goods/services are designed may otherwise affect consumer autonomy, but also the principle of equal treatment. This occurs when digital platforms use recommender systems[29] (i.e., algorithms that provide suggestions about what a user might be interested in) to tailor the results of an online search to each individual (so-called differential ranking). As a consequence, the content (commercial and non-commercial) made available to each consumer is differentiated in light of a number of parameters, including the use of profiling and personalization techniques (see paragraph 2.4.). This practice is widely used in e-commerce and more generally in business-to-consumer transactions in online marketplaces.

The opacity of the criteria used to arrange the results of the online search prevents the user from understanding the logic recommender systems apply and means that the user can be easily manipulated in his or her purchasing choices[30].

2.3. Practices amounting to differential treatment in platform to consumers relations: price differentiation.

Commercial practices involving differential treatment and/or economic discrimination against consumers[31] are a common feature of online markets, which parallel the forms of differentiation that occur in the context of the relations between digital platforms and their business users.

Practices of such a nature include the so-called price differentiation[32], whereby digital marketplace operators are able to offer the same goods and services on a large scale at different prices to each consumer[33].

The practice of price differentiation[34], when based on the inferred (in the online context

---

[29] Rules on recommender systems are included in the new DSA Proposal: Article 2 (o) of the Proposal defines a recommender system as a "fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed".

[30] See D.Paraschakis, Algorithmic and ethical aspects of recommender systems in e-commerce ((2018)) Malmö: http://muep.mau.se/bitstream/ handle/2043/24268/2043_24268%20Paraschakis.pdf?sequence=3&isAllowed=y.

[31] H. Schulte-Nölke, F. Zoll, *Discrimination of the Consumers in the Digital Market*, *Study of the European Parliament*, 2013, 47, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/imco/dv/discrim_consumers_/discrim_consumers_en.pdf.

[32] See OECD, *Personalised Pricing in the Digital Era.* Background Note by the Secretariat, 28 November 2018, available at https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf. See *Consumer market study on online market segmentation through personalised pricing/offers in the European Union* conducted for DG Just by Ipsos, London Economics and Deloitte, June 2018, available at https://ec.europa.eu/info/publications/consumer-market-study-online-market-segmentation-through- personalised-pricing-offers-european-union_en. With regard to differentiated practices occurring in platforms to businesses relations, see the Reports of the *Observatory for the Online Platform Economy* [C(2018), 2393 final], available https://ec.europa.eu/digital-single-market/en/news/commission-expert-group-publishes-progress-reports-online platform- economy.

[33] A. Lindsay, E. McCarthy, *Do we need to prevent pricing algorithms cooking up markets?* (2017) 32(12) *European Competition Law Review*, 533.

[34] O. Bar-Gill, Algorithmic Price Discrimination: When Demand Is a Function of Both Preferences and (Mis)Perceptions (May 29, 2018) 86, University of Chicago Law Review, The Harvard John M. Olin Discussion

as well as in the offline environment) propensity of the consumer to pay, is not per se unlawful in the light of consumer law[35]; it may, however, be illegitimate in some cases, depending on the techniques employed and the ways in which knowledge of the maximum price consumers are willing to pay for a given good or service is acquired and/or exploited by digital platforms. According to some scholars, online marketplaces that apply a differential price must inform consumers in compliance with a principle of transparency[36]. The modernization directive[37] has expressly set forth a duty to provide "where applicable, information that the price has been personalized on the basis of an automated decision-making process"[38], adding that such a duty of transparency is "without prejudice to Regulation (EU) 2016/679, which provides, inter alia, for the right of the individual not to be subjected to automated individual decision-making, including profiling" (see Recital no. 45). Thus, the provision implicitly recognizes not only that businesses are currently able to gain exact knowledge of the individual consumer's maximum propensity to pay for a given good or service[39], but also that the accumulation of data, a necessary prerequisite for

Paper Series, No. 05/2018, Harvard Public Law Working Paper No. 18-32, available at SSRN: https://ssrn.com/abstract=3184533

[35] See European Commission, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, SWD(2016) 163 final, 134. In this regard, the so-called Services Directive (Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market) includes a general prohibition on price discrimination only when it is based on the consumer's nationality and place of residence.

[36] Cfr. P. Hacker, *Personalizing EU Private Law: From Disclosures to Nudges and Mandates*, in *European Review of Private Law*, (2017) 25(3), 651, nonché A. Porat, L. J. Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data,* in Michigan Law Review, (2014) 112(8), 1417. See in this respect, EC (2018), *Consumer market study on online market segmentation through personalised pricing/offers in the European Union*, European Commission, https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf. according to which consumers have a more positive reaction to online personalisation when they are aware that data collection and personalisation is taking place, and also when they can opt out of such practices.

[37] Art. 4 of the modernization directive has inserted into art. 6, par. 1, CRD a letter *e bis).*

[38] See Recital no. 45: "Traders may personalise the price of their offers for specific consumers or specific categories of consumer based on automated decision-making and profiling of consumer behaviour allowing traders to assess the consumer's purchasing power. Consumers should therefore be clearly informed when the price presented to them is personalised on the basis of automated decision-making, so that they can take into account the potential risks in their purchasing decision. Consequently, a specific information requirement should be added to Directive 2011/83/EU to inform the consumer when the price is personalised, on the basis of automated decision-making…". Requiring businesses to disclose personalised pricing practices represents an effective remedy according to the Organisation for Economic Co-operation and Development's Study on Personalised Pricing in the Digital Era (DAF/COMP(2018)13, 20 November 2018, 35 ss.), as long as mandated disclosure procedures are simple, clear and relevant, as opposed to lengthy and complex disclosures that are unlikely to be read by consumers.

[39] "European Data Protection Supervisor. (2015). Opinion No. 7/2015. Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability. Available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/meeting-challenges- big-data_en.

acquiring such knowledge, may take place in violation of the provisions on data protection[40].

2.4.Personalization of advertising and targeting techniques in platform to consumer relations.

Differential pricing is only a manifestation of a broader phenomenon that occurs in online marketplaces, which is not explicitly addressed by existing rules, the so-called personalization[41], i.e. the use of technology to optimize advertising campaigns' efficacy to the highest possible degree. Personalization is the combined effect of multiple technologies, which reinforce each other (such as tracking tools and IoTs' sensors[42], psychographic techniques, which enable psychological attitudes to be inferred from behaviour, image and voice recognition technologies that allow businesses to capture emotional response to advertising and to exploit such knowledge, etc.). Therefore, it has become possible to gain exact knowledge not only about consumer preferences and characteristics, as inferred (on the basis of profiling), but also about (mis)perceptions and vulnerabilities (due to psychological and physiological states) of individuals, as *observed* in real time[43].

Businesses and organizations that use these technologies understand consumers' decision-making better than consumers themselves and, therefore, are able to *coerce* consumers into commercial decisions they would not have taken otherwise. This is made possible by resorting to powerful tools (referred to in the literature as "hypernudges"[44]), consisting in algorithms programmed to self-learn how to exploit vulnerabilities[45].

It is clear that, in such cases, we are faced with practices of manipulation of the consumer who operates in digital markets[46], with the aim of exploiting and even creating new forms of

---

[40] European Data Protection Board, *Guidelines 8/2020 on the targeting of social media users. Version 1.0*, 2 September 2020, available at *https://edpb.europa.eu/our-work-tools/public-consultatio ns-art-704/2020/guidelines-082020-targeting-social-media-users_it*.

[41] Q. André, Z. Carmon, K. Wertenbroch et alii, *Consumer Choice and Autonomy in the Age of Artificial Intelligence*, (2018) 5 *Customer Needs and Solutions*, 8.

[42] See also see Scott R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Texas Law Review, (2014), 95 ss., 117 e 119: "The first Internet of Things problem is the widespread sensor deployment: Internet of Things data will allow us to sort consumers more precisely than ever before". According to the author, the widespread use of third wave technologies (such as the IoT technologies) has made available a greater amount of intimate and personalised data, creating additional personalised targeting opportunities.

[43] C. Burr, N. Cristianini, *Can machines read our minds?* (2019) 29 *Minds and Machines*, 61–494.

[44] K. Yeung, *'Hypernudge': Big Data as a mode of regulation by design* (2017) 20(1) *Information, Communication & Society*, 118

[45] G. Sartor, *Consumer Law and Artificial Intelligence. Challenges to the EU Consumer Law and Policy Stemming from Business' Use of Artificial Intelligence* (n.17) 28: "personalised advertising involves the massive collection of personal data, which is used in the interests of advertisers and intermediaries, possibly against the interests of data subjects. Such data provide indeed new opportunities for influence and control, they can be used to delivers deceitful, or aggressive messages, or generally messages that bypass rationality by appealing to weaknesses and emotions". See J.D. Cohen, *Between Truth and Power. The Legal Constructions of Informational Capitalism* (2019) Oxford University Press.

[46] K. Manwaring, *Emerging Information Technologies: Challenges for Consumers* (April 25, 2017) Oxford University Commonwealth Law Journal (2017) Vol. 17 (2) available at SSRN: https://ssrn.com/abstract=2958514.

vulnerability[47]. Digital consumer manipulation, as this phenomenon is called by the relevant literature, can erode consumer autonomy, limit choice and competition, violate privacy and even compromise personal dignity (when it is successful in persuading consumers to conduct transaction that they would not otherwise have concluded). In the end, the influence of such practices on consumers' decisions might result in overspending, purchasing unrequired goods, financial risks, etc.[48]. It is, therefore, pivotal to determine the "legally permissible levels of transactional exploitation"[49] and find the adequate legal measures of protection.

3.Role played by UCPD rules in tackling the new forms of vulnerabilities arising in the context of platform to consumer dealings.

Consumer law and most notably the legislation on unfair commercial practices can play a role in ensuring that platforms do not cross the thin line between recourse to legitimate forms of persuasion and the exercise of undue influence or even coercion over consumers.

And in fact, under the rules on misleading commercial practices, it is sufficient that the practice (action or omission) employed by the trader induces or is likely to induce the average consumer to take a decision of a commercial nature that the latter would not otherwise have taken. The trader is required to provide clear and transparent information on all elements that, depending on the circumstances, may be decisive for the consumer's informed consent. Interpreters therefore infer from this provision an open number of duties of information, not limited to those provided for by specific provisions. To this end, consumers need to know whether the trader collects their personal data and for what purposes, as well as whether data is collected that is not necessary for the provision of the service and whether, conversely, such data is used for commercial purposes[50] (and/or is passed on to third parties). Accordingly, it is incumbent on the trader to inform if it engages in tracking, profiling and related practices, such as personalized pricing and consumer targeting[51].

With regard to behavioural targeting and personalization techniques, the UCPD provisions against aggressive marketing practices can help to safeguard the consumers' autonomy, provided that some difficulties of interpretation are overcame: i) firstly, regarding the criteria for distinguishing lawful/fair practices from unlawful/unfair ones in a digital environment, especially with respect to the peculiarities of AI applications; ii) secondly, with regard to the way of conceptualising the vulnerability of the consumer.

In this respect, proper interpretation of the paradigm of vulnerable consumer is desirable, considering that according to the Charter of Fundamental Rights of the European Union,

---

[47] European Data Protection Supervisor, *Opinion 3/2018, EDPS Opinion on online manipulation and personal data* (19 March 2018) 22.

[48] G. Sartor, *New aspects and challenges in consumer protection. Digital services and artificial intelligence* (n. 18) 14.

[49] See E. Mik, *The erosion of autonomy in online consumer transactions* (n. 16).

[50] See the Italian Consumer and Market Authority decision fining Facebook Inc. e Facebook Ireland Ltd. for not clearly disclosing the commercial purpose behind the collection and processing of consumers' personal data (https://agcm.it/dotcmsdoc/allegati-news/IP330_chiusura.pdf).

[51] According to the European Commission, the functionality also refers to whether personalization happens (see *Commission, DG Justice Guidance Document concerning Directive 2011/83/EU on consumer rights* (2014), 67: "As appropriate to the product, the following information should be given: . . . Any conditions for using the product not directly linked to interoperability, such as: a. tracking and/or personalization", available at <ec.europa.eu/justice/consumer-marketing/files/ crd_guidance_en.pdf>.).

'Union policies shall ensure a high level of consumer protection' (Article 38). The need for a revision of this notion is much more apparent with respect to the consumer dealing with the complexity of the online environment[52].

With modern personalized marketing techniques, "firms can not only take advantage of a general understanding of cognitive limitations, but they can also uncover and even trigger consumer frailty at an individual level"[53]. Therefore, to protect consumers effectively, consideration should be given to the emergence of new forms of vulnerabilities, other than that those considered by the UCPD' rules (infirmity, age or credulity). Some scholars propose to adopt a more appropriate concept of vulnerability and to focus on the limited ability to deal with business practices; they also highlight the fact that the use of certain persuasive strategies, such as profile based targeting and behavioral targeting, is primarily aimed at turning the average consumer into a vulnerable consumer[54]. However, it is much discussed whether such an outcome can be achieved through proper interpretation of UCPD rules or rather these rules need updating. In this regard, the EU resolution on a strategy for strengthening the rights of vulnerable consumers suggests that the concept of vulnerable consumers should also include consumers in a situation of vulnerability, meaning consumers who are placed in a state of temporary powerlessness resulting from a gap between their individual state and characteristics on the one hand, and their external environment on the other hand[55].

Despite the persisting uncertainty, member States market authorities and EU Institutions interpret/apply UCPD rules in such a way as to take into account not only individual consumers interests but also a broader economic and societal perspective[56]. This tendency is consistent with the fact that practices such as the ones above described encroach upon

---

[52] The average consumer, as the 'reasonably informed, observant and circumspect' consumer, is defined by Recital 18 of the UCPD. See B. Duivenvoorde, '*The protection of vulnerable consumers under the Unfair Commercial Practice Directive*' (2013) 2 *Journal of European Consumer and Market Law* 69-79, 73; J. Trzaskowski, *The Unfair Commercial Practices Directive and Vulnerable Consumers*, paper presented at the 14th Conference of the International Association of Consumer Law (2013), available at http://www.iaclsydney2013.com/

[53] R. Calo, *Digital market manipulation* (2014) 82, *George Washington Law Review*, 995, available at <ssrn.com/abstract=2309703>. The requirements for the average consumer in a digital environment must reflect in some way or other the greater technical and organisational complexity but also the changed nature of digital or digitally-enhanced products, and hence the diminished consumers' ability to deal with that complexity.

[54]E. Mik, *The erosion of autonomy in online consumer transactions*, (2016) 8(1), *Law, Innovation and Technology*, 1, 33, who claims that vulnerability may also be "dynamic state". See H. W.Micklitz, N. Reich, The Court and Sleeping Beauty: The revival of the Unfair Contract Terms Directive (UCTD), (2014) 51 *Common Market Law Review*, 771. See N. Helberger, B.F. Zuiderveen, A. Reyna, *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law* (n.18), 1458, who observe that, in view of the possibility for traders to "target individuals", more legal attention should be paid to the individual characteristics and vulnerabilities.

[55] European Parliament resolution of 22 May 2012 on a strategy for strengthening the rights of vulnerable consumers (2011/2272(INI)). Prepared by the Committee on the Internal Market and Consumer Protection, p. 6. The Resolution recognises that all consumers are susceptible to becoming vulnerable consumers over the course of their lives due to external factors and their interactions with the market

[56] See I. Garaci, R. Montinaro, *Public and Private Law Enforcement in Italy of EU Consumer Legislation after Dieselgate*, (2019) 1 *Journal of European Consumer and Market Law Review*, 29. See, with regard to unfair practices related to the processing of personal data, Italian Competition Authority (Autorità Garante della Concorrenza e del Mercato), decisions PS11112 – *Facebook-Condivisione dati con terzi*, 29 novembre 2018, n. 27432, and PS10601 – *Whatsapp-Trasferimento dati a Facebook*, 11 maggio 2017, n. 26597.

privacy, autonomy and even individual dignity.

Proper governance of online platforms is decisive when it comes to protecting fundamental rights, as recognised by the European Parliament in its resolution on the Digital Services Act and fundamental rights issues[57]. The motto coined by the EU Parliament is: "it is not a matter of ensuring innovations against fundamental rights but, on the contrary, of promoting innovation through a fundamental rights framework".

[57] See the European Parliament resolution on the Digital Services Act and fundamental rights issues (of 20 October 2020, 2020/2022(INI)): according to the EU Parliament the business model currently applied by digital platforms including targeting of individuals based on characteristics exposing physical or psychological vulnerabilities impacts substantially on human dignity and fundamental rights protection.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

The legal qualification of collaborative platforms offering composite services. What consequences for consumer protection?

VIOLA CAPPELLI
Ph.D. Candidate in Law at Sant'Anna School of Advanced Studies of Pisa

Abstract

This paper discusses the legal qualification of collaborative platforms offering composite services, and it aims at identifying a preliminary solution that could ensure a high level of consumer protection to users. The paper argues that collaborative platforms should be considered providers of information society services according to the E-Commerce Directive, without precluding their classification as offline services providers in light of sector regulations.

Moreover, the paper focuses on contractual liability of platforms for non-performance by offline suppliers. The solution suggested is using the criterion of the decisive influence elaborated by the CJEU in Uber and Airbnb cases to define cases where a platform is obliged to compensate consumers for non-performance.

Keywords: collaborative platforms - composite services - information society services - consumer protection - prosumer - E-Commerce Directive - sector regulation - liability for non-performance.

Summary: Introduction. – 1. The main features of the collaborative economy. A legal perspective. – 2. The applicable legal regime to collaborative platforms offering composite services: an overview of the CJEU's case-law and the academic literature. – 3. The legal qualification of collaborative platforms in the light of consumer protection needs. – 4. The allocation of liability for non-performance. The decisive role of platforms in light of the E-Commerce Directive's approach. – 5. The ELI Model Rules on Online Platforms. An overview. – Conclusions.

Introduction.

Collaborative platforms have become increasingly popular in recent years and are disrupting traditional centralized business models of supplying goods and services. Their spread is involving the most different market sectors and has its roots in several technical, social, and economic factors.[1] The technological evolution of mobile devices, systems of online transactions, and geolocation represents the essential context in which collaborative platforms have been developed. At the same time, the idea of sharing unused goods represents a social reaction to an 'overmarketized' society and shows a new environmental consciousness based on the sustainability of consumption.[2] Most importantly, *sharing economy* arises as an alternative economic model and constitutes an answer to the financial crisis and

[1] V Hatzopoulos, S Roma, 'Caring for sharing? Collaborative economy under EU law' (2017) 54 Common Mark. Law Rev. 81.

[2] T Teubner, 'Thoughts on the Sharing Economy' in P. Kommers and others (ed), *Proceedings of the International Conferences on e-Commerce 2014* (2014) <https://www.researchgate.net/publication/285356329_Thoughts_on_the_Sharing_Economy> accessed 03 September 2020.

the resultant unemployment, enabling non-professional actors to profit for monetization of idle capacity.[3]

The chance for strangers to interconnect with each other without traditional intermediaries challenges the vertical and centralized way of conceiving legal relationships between market actors. As a result, the *collaborative economy* raises relevant issues related to the application of existing legal frameworks.[4] More specifically, collaborative platforms that offer composite services – i.e. non-electronic performances through electronic means – are the most difficult to classify and regulate, as shown in cases arising before courts both in the EU and US.[5] Innovative platforms try to avoid the application of rules that impose on offline providers stricter market access requirements than the ones contained in regulations on online services. At the same time, incumbents complain about a disproportionate competitive disadvantage caused by new platforms that offer their same services without the same administrative burdens. For these reasons, regulators, judges, and researchers are seeking to rationalize these issues and strike a balance between the different interests at stake. In doing so, one of the main regulatory objectives should be to figure out solutions able to create a trustworthy environment for consumers.[6] However, this topic is still not thoroughly explored in the literature, except for some authors that have started to investigate the implications of the first CJEU's rulings on the legal treatment of consumers operating in collaborative platforms.[7]

This paper will focus on the dynamic aspect of transactions in collaborative platforms, using the categories of contract law and consumer protection law to preliminarily outline a legal regime for the emerging *collaborative economy*. More specifically, the paper endeavors to solve the issue of the legal qualification of collaborative platforms offering composite services – whether they are providers of information society services within the meaning of Article 2(a) of Directive 2000/31[8] (E-Commerce Directive) or not – in order to identify suitable solutions to ensure a high and uniform level of consumer protection to users. In this context, particular attention will be devoted to transparency requirements and contractual liability for non-performance, considered as the key factors to regulate in order to ensure a trustworthy environment for consumers and to encourage the participation of *prosumers*. To this end, the research will emphasize, from a legal point of view, the role of the technical means by which exchanges are enabled in collaborative platforms. The technological dimension of transactions should be considered the decisive element in the legal assessment because it introduces a high level of legal uncertainty, having a *disruptive* effect on the traditional way of conceiving market relationships for the supply of services or goods. Moreover, embracing this perspective could avoid the fragmentation of the European digital market and guarantee legal certainty to market operators and users that need to know what rules to follow in their transactions.

---

[3] M Böckmann, 'The Shared Economy: It is time to start caring about sharing; value creating factors in the shared economy' (2013) <https://pdfs.semanticscholar.org/a914/b038d4bddca35994f5c2b202c862de22339c.pdf> accessed 10 March 2020.

[4] A Savin, 'Electronic services with a non-electronic component and their regulation in EU law' (2019) 23 J. Internent Law 13.

[5] For an overview of the case-law, S Ranchordas, 'Does Sharing Mean Caring? Regulating Innovation in the Sharing Economy' (2015) 16 Minn. J. L. Sci. & Tech. 413.

[6] M Inglese, *Regulating the Collaborative Economy in the European Union Digital Single Market* (Springer 2019).

[7] MY Schaub, 'Why Uber is an information society service Case Note to CJEU 20 December 2017 C-434/15 (Asociación profesional Élite Taxi)' (2018) 3 EuCML 109; I Domurath, 'Platforms as contract partners: Uber and beyond' (2018) 25(5) MJECL 565.

[8] European Parliament and Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178.

The paper has the following structure. As a point of departure, Section 1 will explore the phenomenon of the spread of collaborative platforms and identify its main relevant features from a legal standpoint. Section 2 will briefly analyze the decisions of the Court of Justice concerning the legal qualification of the two most common collaborative platforms, such as Uber and Airbnb. Then, Section 3 will point out that the application of the 'decisive influence criterion' elaborated by the CJEU does not ensure protection to consumers and create a framework of legal uncertainty in these emerging marketplaces. On this basis, the paper will stress that all collaborative platforms should be considered as providers of information society services, regardless of the level of control exerted on the underlying service and without precluding at the same time their classification as offline services providers. This solution could guarantee the applicability of the E-Commerce Directive as the minimum instrument to assure a common level of protection to consumers operating in the *collaborative economy* context. In addition, Section 4 will investigate whether the approach of the E-Commerce Directive to define platform liability for the user conduct could serve as a regulatory model to establish cases in which collaborative platforms can be considered liable for non-performance by suppliers/*prosumers*. In this respect, it will be highlighted that platform immunity is not a feasible solution, and the decisive influence criterion could play a role in the identification of liability indicators. Finally, Section 5 will offer a preliminary overview of the ELI Report on Model Rules on Online Platforms,[9] devoting particular attention to the suggested model of contractual liability for non-performance.

1. The main features of the *collaborative economy*. A legal perspective.

Collaborative platforms offer a wide range of services, from transportation to sharing rooms, thus creating new opportunities for consumers and enterprises.[10] There is not a universally accepted definition of the *collaborative economy*, and many terms are used to refer to the same concept, such as *peer-to-peer economy, sharing economy, collaborative consumption*. However, in light of the existing literature on the topic,[11] it is possible to identify some key features that represent the lowest common denominator in all these platforms: i) the digital element on which platforms are based; ii) the possibility of offering offline services for non-professional actors on an occasional basis (hence the term *peer-to-peer economy*); iii) the absence of a change of ownership as a result of transactions (the concept of ownership is replaced by the concept of accessibility); iv) the possibility of profiting from monetization of unused goods or idle capacity; v) the platforms' ability to self-regulate their transactions and self-establish the rules that users must follow to continue to participate in the digital life of the community.

The European Commission has rationalized the ideas coming from scholars and enterprises and has given its definition of the *collaborative economy* in a Communication,[12] establishing that 'the term collaborative economy refers to business models where activities

[9] ELI 'Report on Model Rules on Online Platforms' (2016) <https://www.europeanlawinstitute.eu/projects-publications/completed-projects-old/online-platforms/> accessed 03 September 2020.

[10] In 2011 the Time Magazine nominated sharing economy as one of 'ten ideas that will change the world', <content.time.com/time/specials/packages/article/0,28804,2059521_2059717_2059710,00.html>.

[11] J Kassan, J Orsi, 'The LEGAL Landscape of the Sharing Economy' (2012) 27(1), J. Environ. Law Litig.; D Rauch, D Schleicher, 'Like Uber, But for Local Governmental Policy: The Future of Local Regulation of the 'Sharing Economy' (2014) George Mason University Law and Economics Research Paper Series No 15-01, <http://ssrn.com/abstract=2549919>; C Koopman, M Mitchell, A Thierer, 'The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change' (2015) 8(2) JBEL 529; M Cohen, A Sundararajan, 'Regulation and Innovation in the Peer-to-Peer Sharing Economy' (2015) 82 U Chi L Rev 116 <https://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/Dialogue/Sundararajan_Cohen_Dialogue.pdf> accessed 29 June 2020; V Katz, 'Regulating the Sharing Economy' (2015) 30(385) BTLJ 1068.

[12] *A European agenda for the collaborative economy* COM(2016) 356 final Commission Communication [2016] OJ L 119 .

are facilitated by collaborative platforms that create an open marketplace for the temporary usage of goods or services often provided by private individuals'. The Commission Communication has clarified that platforms offering composite services generally involve three main actors: i) the providers of the underlying service, that can act as professional actors or on an occasional basis; ii) the users of these services; iii) the online platform acting as an intermediary that provides market operators with the digital interconnection needed to facilitate their exchanges. The presence of these three actors has some consequences on the way of understanding traditional two-party contractual relationships. Indeed, in the *collaborative economy* context, contractual interactions should be conceived as a triangle network: a provider enters into a contract with a user for the supply of the underlying service; at the same time both the provider and the user enter into a contract with the platform to use the intermediation service that allows them to digitally interact. Moreover, the Commission specifies that transactions in collaborative platforms can be carried out for-profit or not-for-profit and generally do not involve a change of ownership. This is because parties are interested in the temporary use of a good (an apartment) or need to use a service for a limited time (transportation), so they only need the possibility of accessing to a service or a good, and not acquiring property rights on them. For all these reasons, some authors classified the *sharing economy* as a regulatory *disruption*,[13] able to have drastic implications for the current legal categories because it is based on a kind of innovations that 'goes beyond improving existing products; it seeks to tap unforeseen markets, create products to solve problems consumers don't know they have, and ultimately to change the face of the industry'.[14]

For the purposes of the present article, there are two most crucial features to take into account to ensure the optimum level of protection to consumers in collaborative platforms, namely the overlapping of the two layers of market relationships, the digital one and the offline one, and the presence of a new category of market actors, the *prosumers*, those subjects that offer their service non-professionally. On the first point, at the digital level, consumers and suppliers can interact and conclude their transactions through the intermediation service offered by platforms. Likewise, the offline dimension concerns the offering of the underlying services that cannot be digitized, such as transportation or provision of accommodations. These two layers are inextricably interconnected in every collaborative platform, and this aspect causes many issues associated with the identification of the applicable regime, as the CJEU case-law has shown. However, as discussed below, the twofold dimension of collaborative platforms should not be simplified, but enhanced by judges and regulators, because it represents the context where consumers interact and, therefore, where it is necessary to conceive legal remedies for their protection. Considering collaborative platforms only as digital intermediaries or otherwise only as offline provides would mean ignoring their dual nature, which corresponds to two different sets of rules that, in turn, pursue two different regulatory objectives.

On the second point, the chance for non-professional actors to offer services and goods challenges the traditional *business-to-consumer* (B2C) model, on which the regulation of goods and services supply is based. According to the B2C model, suppliers operate in the market as professional actors and, for this reason, are obliged to apply transparency requirements and specific rules on contracts to fill the information asymmetry of consumers. In the *sharing economy* context, subjects that act as users should maintain their rights as consumers, but

[13] V Katz, 'Regulating the Sharing Economy' (n 11) 1092.

[14] N Katyal, 'Disruptive Technologies and the Law' (2014) 102 Geo. LJ 1685. On the meaning of the expression 'disruptive technology', see CM Christensen, 'The Innovator's Dilemma – When New Technology Causes Great Firms to fail' [1997] Harv. Bus. Rev.

subjects acting as suppliers could hardly ensure consumer protection to users with all the existing tools provided for in the law. This is why the allocation of liability in collaborative platforms represents a serious problem from a consumer protection law standpoint: prosumers are not able to ensure legal protection to users and to pay compensation, and the platform has formally no role in the supply of the underlying services. As discussed below, we can conclude that, in the process of allocation of liabilities, legal solutions should be designed in light of the triangular interactions of market actors by emphasizing the role of the digital platform, which could be decisive also in the provision of offline services.

2. The applicable legal regime to collaborative platforms offering composite services: an overview of the CJEU's case-law and the academic literature.

2.1. The Uber case and the Airbnb case.

The first step to address the problem of the legal framework applicable to collaborative platforms is exploring the case-law of the Court of Justice concerning the legal qualification of Uber and Airbnb.

In *Asociación Profesional Elite Taxi v Uber Systems Spain SL*,[15] a Spanish taxi company started legal proceedings against Uber, seeking a prohibition of its transport activities. This company claims that Uber offers a transport service without being subject to all required applicable authorizations and rules on traditional taxi services, and these activities amount to misleading practices and acts of unfair competition. So, the question referred to the Court was whether Uber services could be classified as transport services within the meaning of Article 58(1) TFEU and, therefore, excluded from the scope of Article 56 TFEU, Directive 2006/123 (Service Directive)[16] and Directive 2000/31, or whether they could be considered online intermediation services, and, so, covered by the aforementioned rules. The Court first notes that the intermediation service of matching a non-professional driver with a passenger is, in principle, a separate service from a transport service consisting of the physical act of moving persons from one place to another and that each of these services is subject to different directives. Second, the Court recognizes that an intermediation service that, through a smartphone application, enables the transfer of information concerning the booking of a transport service between a passenger and a non-professional driver meets, in principle, the criteria for classification as an 'information society service' within the meaning of Article 2(a) of Directive 2000/31. Nevertheless, the booking service offered by Uber must not be classified as an information society service, but as 'a service in the field of transport', because of the active role exercised by the digital platform on the substantive service conditions. In this regard, the intermediation service forms an integral part of an overall service whose main component is the transport service. According to the Advocate General Szpunar's Opinion,[17] this digital interconnection activity is not economically independent but exerts a pervasive influence on the conditions under which the transportation service is provided by non-professional drivers, such as determining the maximum fare, exercising a certain control over the quality of the vehicles, the drivers and their conduct. For this reason, Uber services cannot be considered as information society services, and the effects of the E-Commerce Directive must be restricted to composite services in which the electronic element is

[15] Judgement of 20 December 2017, *Asociación Profesional Elite Taxi v Uber Systems Spain SL,* C-434/15, EU:C:2017:981.

[16] European Parliament and Council Directive 2006/123/EC of 12 December 2006 on services in the internal market [2006] OJ L 376.

[17] Opinion of Advocate General Szpunar delivered on 11 May 2017, *Asociación Profesional Elite Taxi v Uber Systems Spain SL*, C-434/15, EU:C:2017:364.

independent from the non-electronic one. In summary, although online and offline services are, in principle, subject to own regulations, the criterion to identify the correct applicable regime is to verify whether the two services are economically independent. If so, the E-Commerce Directive applies to the electronic services, while the offline service remains subject to its regulation. Otherwise, it is necessary to establish which is the dominant element, and, therefore, apply the E-Commerce Directive when the electronic element is dominant, and the offline regulation when the non-electronic one prevails.

The Court again applies the decisive influence criterion to identify the legal regime suitable for regulating Airbnb services,[18] but it arrives at the opposite solution. Advocate General Szpunar[19] clarifies the criteria to establish whether collaborative platforms services should be classified as information society services. As the Uber case has shown that the applicable regime to composite services depends on the level of control exercised by the electronic platform on the non-electronic component, then the intermediation service offered by Airbnb – consisting of compiling of offers using a harmonized format, coupled with tools for searching for, locating and comparing those offers – constitutes an autonomous and economically independent service. These activities cannot be regarded as merely ancillary to an overall service coming under a different legal classification, namely provision of accommodation services. Moreover, hosts and guests can use many other channels to obtain accommodation services, so Airbnb is not indispensable to provide this offline service. According to the Court, it is not possible to infer that Airbnb offers accommodation services from the mere fact that it competes with traditional channels offering the same services. In conclusion, unlike Uber, the electronic element of Airbnb services is autonomous from the non-electronic one and does not exert a decisive influence on the conditions of the offline performance. Therefore, Airbnb can be considered a provider of information society services and benefit from the most favorable rules of the E-Commerce Directive.

Thus, the question in both cases was whether it is possible to consider collaborative platforms offering composite services as providers of information society services in the light of the E-Commerce Directive, or whether they are comparable to traditional offline companies of the underlying service. In the former case, they would benefit from the principle of freedom to provide information society services in the EU; in the latter, they would be subject to market access requirements imposed by national regulations within the minimum harmonization limits contained in the Service Directive, where applicable (for instance, not in the case of transportation).[20] By laying down the decisive influence criterion, the Court adopts a case-by-case approach aiming at excluding the applicability of the E-Commerce Directive in cases in which collaborative platforms determine the contractual conditions of the substantive service offered and control the relevant underlying market. According to the Court interpretation, the existing European legislation would be *de facto* inadequate to regulate the *collaborative economy* phenomenon. Indeed, applying the criterion of the decisive influence in the particular case of platforms offering transportation services means delegating the regulatory power to the Member States, which can decide for themselves to allow or prohibit Uber. The result of this approach is fragmentation that involves not only the European internal market for the same offline service but also the harmonization of the Digital Single Market as a whole, because of the variety of underlying services, governed by own regulations, that online platforms offer.

---

[18] Judgement of 19 December 2019, *Airbnb Ireland*, C-390/18, EU:C:2019:1112.

[19] Opinion of Adovcate General Szpunar delivered on 30 April 2019*, Airbnb Ireland*, C-390/18, EU:C:2019:336.

[20] On the limited capacity of the Service Directive to protect providers of a composite service where the E-Commerce Directive is not applicable, A Savin, 'Electronic services with a non-electronic component and their regulation in EU law' (n 4).

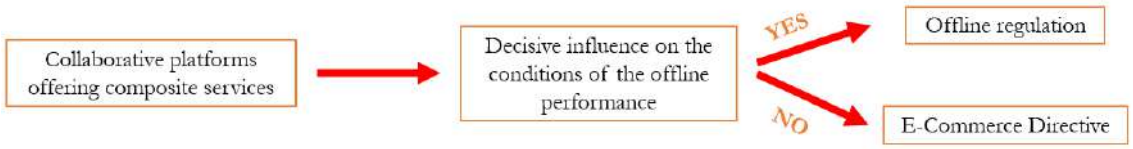


Fig. 1. The impact of the criterion of the decisive influence elaborated by the Court of Justice on the applicable legal regimes.

2.2. The Communication of the European Commission and the reactions from academia.

It should be highlighted that the aforementioned CJEU's decisions have completely ignored the guidelines established by the Commission Communication on the *collaborative economy*.[21] The Commission adopts a comprehensive approach that takes into consideration the specific features of *collaborative economy* business models and, in particular, the way in which these platforms carry out their activities. On this basis, it points out that collaborative platforms are first of all providers of information society services. However, in some particular cases, they may also be considered as providers of the underlying services and be subject to the relevant sector-specific regulation, including authorizations and licensing requirements. The Commission lists three criteria, based on the level of control exerted on relationships between users and underlying suppliers, to determine whether a platform can also be considered as a provider of the offline service: i) the control over the price of transactions. This criterion is met only when collaborative platforms set the final price that users have to pay and not when the platform merely recommends a price or the offline provider is free to adapt the price set by the platform; ii) the control over setting terms and conditions of the underlying service. This criterion is met when the platform determines the terms and conditions that govern the contractual relationships between offline providers and users; iii) the ownership of the key assets used to provide the underlying service. This criterion means that the platform uses its own assets to provide not only the online interconnection but also the underlying service. When these three criteria are all met, a platform should reasonably be considered as a provider of the underlying service, as well as an information society service provider, and be subject to the relevant regulation.[22] However, the CJEU did not refer to these criteria to integrate the decisive influence standard and, most importantly, did not recognize the general twofold nature of the composite services offered by collaborative platforms, which should be considered information society services in every case and also offline services in some cases, according to the Commission Communication.

Many authors have commented on the legal and regulatory implications of these judgments on the *collaborative economy*. In particular, they have investigated whether the criterion elaborated by the Court could strike a fair balance between the growth of innovative business models and the needs of protection of incumbents that are subject to strict market access requirements.[23] In this regard, it must be said that the Uber and Airbnb cases have

[21] C Cauffman, 'The Commission's European Agenda for the Collaborative Economy – (Too) Platform and Service Provider Friendly?' (2016) 5 Common Mark. Law Rev. 235.

[22] *A European agenda for the collaborative economy* 7: 'Generally speaking, the more collaborative platforms manage and organize the selection of the providers of the underlying services and the manner in which those underlying services are carried out — for example, by directly verifying and managing the quality of such services — the more apparent it becomes that the collaborative platform may have to be considered as also providing the underlying services itself'.

[23] D Geradin, 'Online Intermediation Platforms and Free Trade Principles – Some Reflections on the Uber Preliminary Ruling Case' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2759379> accessed

not been welcomed by commentators. Most of all, they have criticized the restrictive approach adopted by the Court, according to which the way platforms conduct their business is irrelevant if the non-electronic service appears predominant. This approach jeopardizes the principle of legal certainty in the regulation of the *collaborative economy*. Indeed, collaborative platforms offer the most different underlying services; as a result, following the factual approach of the Court risks creating a fragmented scenario of different applicable legal frameworks and undermining the completion of the European Digital Market.[24] On the other hand, the solution of the Court does not reach the dual objective of protecting the freedom of innovative platforms to offer services and, at the same time, ensuring that these platforms comply with offline regulatory requirements provided to correct market failures, and not to prevent market access for competitors.[25] In this context, a comprehensive attempt to rationalize the legal implications of these judgments in the field of consumer protection is still missing. So, after analyzing the impact of the decisive influence criterion on the legal treatment of consumers, this paper will focus on what could be the most effective legal framework to apply in order to ensure a minimum level of consumer protection in collaborative platforms.

3. The legal qualification of collaborative platforms in the light of consumer protection needs.

3.1. The harmonizing role of consumer provisions in the E-Commerce Directive.

At the end of the day, the substantial result of the Court of Justice interpretation in the Uber case is ruling out the application of the E-Commerce Directive in the *sharing economy* context[26] and jeopardizing its harmonizing role by the introduction of a further element of legal uncertainty. According to the Court approach, the electronic component enabling collaborative platforms services is completely irrelevant in defining the applicable regime in so far as the offline component is dominant over all other aspects. Therefore, many collaborative platforms will be generally classified as underlying services providers, without the opportunity to benefit from the more favorable regime of the E-Commerce Directive.

As a result, this solution could seriously affect consumers.[27] The E-Commerce Directive contains a detailed list of the information to be provided to users, including the name and the address of the service provider (art. 5), and the requirements to provide commercial communications (art. 6). In addition to these transparency requirements, the Directive regulates the treatment of online contracts, including the information to give to the users before the order is placed, such as the different technical steps to follow to conclude the contract and the technical means for identifying and correcting input errors (art. 9–11). It appears clear that qualifying collaborative platforms only as providers of the underlying services would mean not enforcing these rules and, therefore, diminishing protection instruments tailored to consumers that operate in a digital environment. Even considering

9 March 2020; P Hacker, 'UberPop, UberBlack, and the Regulation of Digital Platforms after the Asociación Profesional Elite Taxi Judgment of the CJEU' (2018) 14 Eur Rev 80; M Finck, 'Distinguishing internet platforms from transport services: Elite Taxi v. Uber Spain' (2018) 55 Common Mark. Law Rev. 1619; C Busch, 'The Sharing Economy at the CJEU: Does Airbnb pass the 'Uber test'? Some observations on the pending case C-390/18 – Airbnb Ireland' (2018) 4 EuCML 172; A De Franceschi, 'Uber Spain and the Identity Crisis of Online Platforms' (2018) 1 EuCML 1.

[24] M Inglese, *Regulating the Collaborative Economy in the European Union Digital Single Market* (n 6) 34.

[25] D Geradin, 'Online Intermediation Platforms and Free Trade Principles' (n. 23).

[26] M Inglese, *Regulating the Collaborative Economy in the European Union Digital Single Market*' (n 6) 34.

[27] MY Schaub, 'Why Uber is an information society service' (n 7); C Busch, 'The Sharing Economy at the CJEU' (n 23).

other consumer protection provisions still applicable, such as the Directive on Unfair Contract Terms, the Directive on Unfair Commercial Practices, and the Consumer Right Directive, the impossibility of classifying active platforms like Uber as information society services providers would result in detrimental effects on the peculiar protection needs of consumers engaging in online transactions.

All things considered, collaborative platforms services should always be considered information society services, without precluding their simultaneous classification as offline services, such as transportation or provision of accommodation service. As a result, active platforms offering composite services should be subject to the E-Commerce Directive and, at the same time, to the relevant rules applicable to underlying services, which are the Service Directive, where applicable, and the Member States regime, including authorizations and license requirements.[28] Although market access requirements for offline services could affect the freedom of collaborative platforms to provide online services, it must be said that, according to the Service Directive, access requirements have to comply with the principles of non-discrimination, necessity, and proportionality. On the contrary, making the enforcement of the E-Commerce Directive subject to the decisive influence check would lead to an unjustifiable unequal treatment between consumers operating in active collaborative platforms – they would not benefit from the legal protections of the Directive – and consumers that interact in more neutral collaborative platforms. On the surface, it might seem that not applying the E-Commerce Directive could have adverse effects only on collaborative platforms business because they cannot benefit from the principle of freedom to provide information society services, and, therefore, are subject to strict requirements laid down for preventing market failures. However, closer examination reveals that, in the end, platforms could profit from the exemption to the E-Commerce Directive since they do not have to comply with information requirements and rules governing online contracts.[29]

3.2. The triangular structure of contractual relationships in collaborative platforms. The role of the technological layer.

In the end, considering platforms services at the same time as information society services and offline services could ensure a fair balance between incumbents and newcomers and, most importantly, a high level of protection for digital consumers of offline services. Thus, collaborative platforms can benefit from the principle of freedom to provide information society services but, at the same time, are required to comply with the transparency requirements and the rules applicable to online contracting. On the contrary, following the approach of the CJEU would mean, first of all, fragmenting the area of effectiveness of the E-Commerce Directive and, second, making the application of consumer provisions conditional to an uncertain and difficult case-by-case assessment based on the level of

[28] In this regard, the control exerted by the online platform on the substantive service should be a benchmark for determining not whether the E-Commerce Directive is applicable, but rather under what circumstances the platform is liable for nonperformance by suppliers/users (§ 5).

[29] MY Schaub, 'Why Uber is an information society service' (n 7) 114: 'The judgement essentially limits the scope of the ecommerce Directive to independent or neutral platforms, that is to say platforms that have no relation or interference with the users that offer their goods or services via the platform, nor with the contracts concluded via the platform or the provision of the offline services. It could mean, for example, that if […] an online platform where cleaners can offer their cleaning services screens and selects the cleaners and sets certain conditions for the performance of the cleaning service, this active role can lead to an exclusion of the platform from the applicability of the directive. At first sight this may seem to be to the detriment of the active platform, because this entails that it cannot rely on the principles relating to the freedom to provide information society services, but the platform in the end also profits as it does not need to comply with the transparency requirements and the rules related to online contracting'.

influence exerted by the platform on offline performances. In such a way, there would not be a minimum level of protection for users operating in these platforms, and consumers would risk losing some basic contractual rights specifically designed to protect them in a digital environment. To avoid this, it should be noted that the legal situation of consumers operating in collaborative platforms is the same and, therefore, rights ensured to a passenger using Uber should be no different from the ones guaranteed to a consumer who rents an apartment on Airbnb. In both cases, consumers are parties of a broader contractual relationship, which, in turn, consists of three different contracts according to a triangular scheme: i) the contract between consumers and the platform, that concerns the provision of the digital interconnection service; ii) the contract between the platform and providers, which allows the latter to offer their offline services through the digital interconnection provided by the platform; iii) the contract between a provider and a consumer, concerning the offline service.

The platform is at the core of this triangular scheme because it constitutes the essential intermediary to connect consumers and providers and allow the communication between them. Indeed, it is the digital layer that enables non-professional actors to offer their services on an occasional basis and challenges traditional centralized business models. So, the distinctive feature of the *collaborative economy* is how the service is provided. It is the technological means that determines the new market structure, and, therefore, has some consequences on the way of conceiving legal relationships. The mere fact that the underlying service is provided by a digital platform makes it not comparable with the same service provided by traditional offline channels. Regardless of the level of control exerted by the platform on the underlying activity and its conditions, what matters and distinguishes traditional services from collaborative services is that consumers rely on the intermediation activity carried out by the digital platform.

The legal interactions of consumers and providers with the platform give rise to two autonomous contracts, that are different from the contract on the offline service and must comply with the requirements enshrined in the E-Commerce Directive. The online contracts (consumers-platform and platform-providers) and the offline contract (consumers-providers) should not be seen in a conflictual relationship. It is not necessary to identify the dominant element – electronic or not electronic – to rule out the application of the E-Commerce Directive in one case, or the underlying service regulation in the other case, as argued by the Advocate General Szpunar. On the contrary, these contracts are integral parts of a broader triangular agreement that requires parties to provide two different services, the offline one and the online one, subject to two different legal frameworks. As a result, consumers should benefit from all the legal guarantees provided for in the E-Commerce Directive.

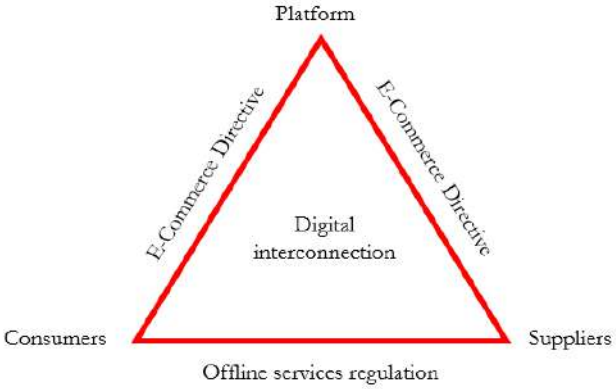


Fig. 2. Legal relationships in active collaborative platforms and the applicable regimes.

In a nutshell, the decisive criterion to identify the applicable legal regime to innovative platforms offering composite services should be conceived in the light of the technical means by which the service is provided. Considering *peer-to-peer* platforms in their twofold role as online intermediaries and offline providers leads to rethinking the traditional way to regulate contractual relationships in the market. From the perspective of ensuring a smooth level of consumer protection and a harmonized Digital Single Market, all that matters is how the performance is provided, not its substance itself. This does not mean that the regulation on underlying services is irrelevant. On the contrary, the offline aspect could have a decisive role in guaranteeing those market access requirements that prevent market failures (for instance, information asymmetry and distortions of competition). However, it is necessary to conceive instruments of legal protection at a higher level, in such a way that the variety of offline services provided in the context of the *collaborative economy* does not result in an attempt to jeopardize legal guarantees for consumers. To this end, the digital element underlying the *collaborative economy* plays a crucial role, leading to enforcing the application of the E-Commerce Directive as the minimum instrument to ensure consumer protection in online platforms.

4. The allocation of liability for non-performance. The decisive role of platforms in light of the E-Commerce Directive's approach.

In light of the dual nature of collaborative platforms, the resulting topic to explore concerns the allocation of liability for non-performance by suppliers of offline services. As previously said, the contractual role of platforms should be distinguished from the legal relationships between suppliers and consumers concerning offline activities. Therefore, platforms could not be held contractually liable in principle for all accidents resulting from the non-adequate performance of underlying transactions. At the same time, regulatory burdens that are traditionally on offline service providers should be revised, because their relationship with consumers in digital platforms cannot be compared with the one they have in traditional offline transactions. All things considered, liability rules should be rethought in light of the different actors involved, thus determining criteria to define cases where a platform could be held liable for non-performance of the underlying service, or where this liability rests on offline suppliers. In this respect, the active role of the platform in defining contract terms could be decisive.

Although the underlying service is almost always provided by suppliers, platforms often act not as mere intermediaries but as the actual suppliers when they conclude the contract with consumers. Here, the platform assumes the economic risk of *collaborative* operations and defines the content of the offline contract by establishing the terms and the standards that providers must meet to offer the performance. For these reasons, some authors define the action of these platforms as a form of 'remote control' over the contractual relationship between consumers and suppliers, consisting, for instance, of providing payment services or reputation systems.[30] In these cases – that are the vast majority in the *sharing economy* context – the main question is, therefore, whether and to what extent it is possible to hold the platform as the liable subject for the non-performance of the providers' obligations, and eventually, what are the applicable rules.

To this end, the approach adopted by section 4 of the E-Commerce Directive on 'Liability on intermediary service providers' could suggest the appropriate solution. Articles 12-15 contain the safe harbors' provisions and specify that there is not a general obligation on online providers to monitor the information which they transmit and store or a general

[30] C Busch, A Wiewiórowska, 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law?' (2016) 1 EuCML 3.

obligation to seek actively facts or circumstances indicating illegal activity.[31] Although these provisions have been applied mainly with regard to infringements of intellectual property and personality rights and are not meant for the *collaborative economy* context, it should be further investigated whether the same approach of the E-Commerce Directive could be adopted to regulate platform liability for non-performance by suppliers.

Without going into the specific content of these provisions, it should be stressed that the Directive recognizes that a form of unmitigated platform immunity could not be an appropriate solution. Therefore, it introduces liability for user conduct only when platforms have an active role in the transmission or storage of information (*mere conduit, caching* and *hosting*) or, more generally, when they have control over the activities carried out within platforms themselves, by specifically identifying the relevant cases. In principle, platforms should not be held liable for suppliers' conduct as long as their actions do not correspond to the situations referred to in articles 12-15.

The same regulatory approach could be useful also to define whether platforms should be held liable for non-performance by suppliers and, therefore, to determine the objective exceptions under which platforms' immunity fails. Upon further research, it seems that the CJEU's criterion of the decisive influence could be applied to establish these cases, rather than to exclude the applicability of the E-Commerce Directive. It would be possible to introduce a sort of joint liability of the platform in cases where it exerts a decisive influence over the conditions under which the offline service is provided by suppliers, for instance when it determines at least the maximum fare; when it receives that amount from the user before paying part of it to the supplier; when it exercises a certain control over the quality of the means by which the services are provided. In this respect, the criteria drafted by the European Commission could play a role in preliminarily defining the relevant level of control exerted such that the platform should be held liable for non-performance by suppliers. If the platform i) sets the final price, ii) sets the terms and the conditions of the offline performance, and iii) owns the key assets used to provide the underlying service, there are strong indications of its control over the underlying service. In other words, in these cases, the platform objectively bears all significant economic chances and risks of the transaction as a traditional contractual partner and, therefore, it should be at least jointly liable with suppliers in case of non-performance. Obviously, these criteria are not exhaustive, and they do not need to be cumulatively present but, if several or all are present in such a way that they show the economic and contractual preeminent role of the platform in the internal relationship between offline suppliers and consumers, this could justify the joint liability of the platform.

To sum up, the criterion of the decisive influence, as elaborated by the Court of Justice and if redesigned in light of the Commission Communication, should play its role not in

[31] More specifically, article 12 states that service providers are not liable for the information transmitted on the condition that i) they do not initiate the transmission; ii) do not select the receiver of the transmission; iii) do not select or modify the information contained in the transmission. As regards the temporary storage of information (art. 13), platforms that just transmit in a communication network information provided by a recipient of the services (caching) are not liable in so far as i) they do not modify the information; ii) comply with conditions on access and iii) rules regarding the updating of the information; iv) do not interfere with the lawful use of technology to obtain data on the use of the information; v) act expeditiously to remove or to disable access to the information as soon as they obtain actual knowledge of its removal or disablement of access at the initial source or by a court. Finally, according to article 14, platforms offering a storage service of information provided by a recipient of the services (hosting) are not liable for the information stored, on the condition that i) they do not have actual knowledge of illegal activity or information nor are aware of facts and circumstances from which the illegal activity or information is apparent; ii) upon obtaining such knowledge or awareness, they act expeditiously to remove or disable access to the information. In any case, platforms, when providing information transmission or storage services, do not have a general obligation to monitor (art. 15).

identifying cases in which the E-Commerce Directive is applicable (all collaborative platforms should be subject to this Directive), but rather in selecting cases in which the platform is liable for non-performance of the contract between consumers and suppliers.

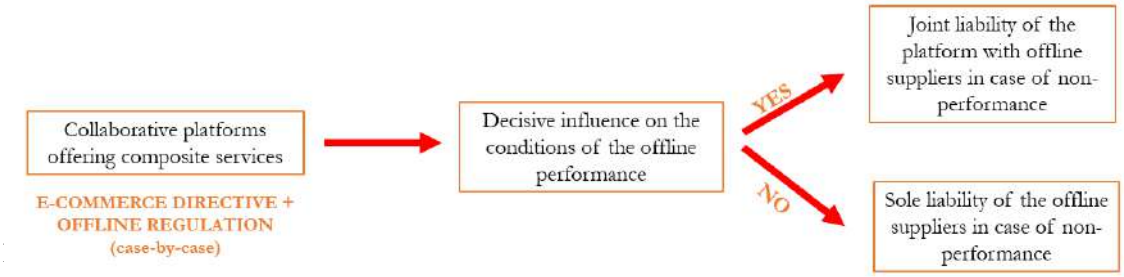


Fig. 3 The use of the decisive influence criterion as a means to select cases in which the platform is jointly liable for non-performance of the contract between consumers and suppliers.

Still, holding the platform jointly liable for non-performance by suppliers is also a more coherent solution with the philosophical assumption behind the concept of the *sharing economy*, based on the idea of empowering and enabling consumers to become prosumers. The non-professional nature of prosumers could be an obstacle to the rise of the *sharing economy* if platform participants alone were held liable for non-performance. Prosumers rely on the platform precisely because they do not have the complex legal and financial structure required to independently offer their services, so allocating the entire liability on them would mean preventing their participation in these innovative marketplaces. At the same time, liability only on prosumers would create an untrustworthy environment for consumers, discouraging them from using services offered by these platforms. On the contrary, the introduction of a form of joint liability of the platform could be the most suitable solution not only for stimulating the rise of *prosumerism* in the *collaborative economy* but especially for ensuring the enforcement of consumers' rights. From this point of view, consumers could claim damages directly from the platform and be sure to obtain compensation; then, at a later stage, the platform and the defaulting supplier could regulate their internal relationships and decide how to allocate these compensation costs.

In conclusion, it should be said that the current regulatory instruments provided for in the law could stimulate and enrich the legal debate on the optimal way to ensure a high level of consumer protection in the process of the allocation of liabilities for non-performance. The technological structure underpinning the *collaborative economy* consists of platforms that enable peers to interconnect with each other and define the content of offline contracts. Precisely for these reasons, platforms should be considered the regulatory units on which legislators, judges, and scholars should focus their attention. Allocating liabilities for non-performance only on suppliers would mean ignoring the complex triangular structure of the *collaborative economy*, and the key role carried out by platforms in transactions. As a result, this would lead to diminishing instruments of protection for consumers because the right to obtain compensation would become more uncertain. On the contrary, using the criterion of the decisive influence to define cases where a platform is obliged to compensate consumers for non-performance could be the most balanced solution to ensure the legal protection of all the interests at stake.

5. The ELI Model Rules on Online Platforms. An overview.

Finally, a brief overview of the *Model Rules on Online Platforms* outlined by the European Law Institute could be useful to rationalize what has been said in this paper and indicate the next steps. These Model Rules contribute to the debate about the convenience of an action

to regulate the changes in the Digital Single Market caused by the rise of the *collaborative economy* and represent the latest version of the Discussion Draft of a Directive on Online Intermediary Platforms, which was drawn up by the Research Group on the Law of Digital Services in 2015 and 2016.[32] This document adopts a *de iure condendo* approach, introducing new harmonization measures, with the aim of, on the one hand, avoiding the risk of stifling innovation and, on the other hand, ensuring basic values, such as consumer protection and fair competition.

First of all, Model Rules define services offered by platforms as information society services (art. 2) and include in this definition not only platforms that exercise control over their digital environment but also mere intermediary platforms, that identify relevant suppliers or direct customers to those suppliers' websites or contact details (art. 1). Most importantly, these Rules regulate the allocation of liabilities, providing that in the case of a violation of Article 13, 'the customer can exercise the rights and remedies available against the supplier under the supplier-customer contract also against the platform operator' (art. 19). In particular, art. 13 imposes on platforms the duty to inform consumers, before the conclusion of the offline contract, that they will be entering into a contract with a supplier and not with the platform. Therefore, responsibility *ex* art. 19 is justified 'by the fact that the platform operator did not fulfil its own duty to inform'.[33]

In addition to these transparency requirements, platforms are liable for non-performance of supplier if the customer can reasonably rely on the platform operator having a predominant influence over the supplier (art. 20). To this end, there are some criteria to be considered in assessing whether a consumer can reasonably rely on the platform operator's predominant influence over the supplier, that are a) the supplier-customer contract is concluded exclusively through facilities provided on the platform; b) the platform operator withholds the identity of the supplier or contact details until after the conclusion of the supplier-customer contract; c) the platform operator exclusively uses payment systems which enable the platform operator to withhold payments made by the customer to the supplier; d) the terms of the supplier-customer contract are essentially determined by the platform operator; e) the price to be paid by the customer is set by the platform operator; f) the marketing is focused on the platform operator and not on suppliers; g) the platform operator promises to monitor the conduct of suppliers and to enforce compliance with its standards beyond what is required by law. It seems that these criteria represent a specification of the decisive influence benchmark, as outlined by the CJEU in Uber and Airbnb cases. However, the ELI Rules implement these criteria not to qualify the platform as a provider of information society services or as an offline services provider, but only to determine when a platform is jointly liable with the supplier for non-performance. Taking into account that collaborative platforms almost always have a key role in the underlying supply contract, the application of the predominant influence criterion could allow consumers to benefit not only from the monitoring function performed by platforms but also from their capability of compensating for damages.

The earlier Draft Directive and these Rules represent a great result in the harmonization of the complex topic of liability and try to rationalize the most relevant legal issues. However,

[32] Research group on the Law of Digital Services, 'Discussion Draft of a Directive on Online Intermediary Platforms' (2016) 4 EuCML 164.

[33] ELI 'Report on Model Rules on Online Platforms' (n 9), Comments on art. 19: 'The CJEU case C-149/15 (Wathelet) shows that in certain circumstances in which the consumer can easily be misled in light of the conditions in which the sale is carried out, eg leading the consumer to believe that the platform operator is the owner of the good, liability can be imposed on an intermediary'.

some aspects are still unclear. More specifically, the Rules do not explain the relationship between the transparency requirement contained in art. 13 (in conjunction with art. 19) and the predominant influence criterion of art. 20. If the platform clearly informs the customer that his actual counterpart is only the offline supplier, but, at the same time, it has a predominant influence over the supplier based on the terms of the supplier-platform contract, the platform should be considered in any case liable for non-performance. The lack of coordination between these two rules raises a fundamental question: if the platform determines, in a prominent manner, the content of the offline contract, could the mere fact that the platform itself has clarified to consumers its apparent passive role exempt it from liability? This uncertainty could jeopardize the effectiveness of the predominant influence criterion and weaken consumer protection mechanisms in case of failures and non-performance. The paradoxical result of art. 13 would be that platforms could always inform consumers on their passive role and, in this way, avoid liability even if they act as the actual supplier of the service by exerting decisive influence over the terms of the offline contract.

Still, as abovementioned, art. 20 introduces the criterion of predominant influence to determine the cases in which platforms can be considered liable for suppliers' non-performance. As noticed by some authors, this rule introduces a form of reliance liability because the predominant influence is not assessed 'in a strict objective manner but according to the reasonable understanding of the customer'.[34] This subjective approach could affect consumers, especially in C2C platforms, where they can also operate as suppliers (*prosumers*) offering offline performance in a non-professional manner. In these platforms, consumers directly enter into a contract with other consumers acting as suppliers: these prosumers are not able to ensure legal protection and compensation rights to other consumers precisely because of their non-professional nature. Nevertheless, according to art. 20, the platform could be held liable only when the relevant circumstances of its predominant influence are apparent to consumers *ex-ante* in such a way that they can rely on the role of the platform as their actual counterparty. However, consumers cannot have a comprehensive understanding of the internal agreement between the platform and the supplier. Thus, designing a system of allocation of liabilities based on the *ex-ante* knowledge of consumers could not be the best solution to ensure a framework of legal certainty for collaborative platforms.[35] If consumers do not rely on the platform's predominant role because, for instance, the platform has clarified its merely intermediary function, but the platform has – on the basis of its internal agreement with suppliers/prosumers – a decisive influence on the offline performance according to the criteria of art. 20, it is difficult to see why the platform should not be held liable for non-performance. The criteria listed in art. 20 should be interpreted not according to the subjective standard of reliance, but in light of the objective circumstance – justified on the basis of the agreement between the platform and the supplier – that the platform

[34] F Maultzsch, 'Contractual Liability of Online Platform Operators: European Proposals and Established Principles' (2018) 3 European Review of Contract Law 209.

[35] ibid 238: 'The mere idea of reliance liability cannot explain why the reasonable confidence of the customer in a predominant influence of the platform operator on the supplier should nonetheless justify a performance responsibility of the former in such a case. If one follows the line of argument developed by the majority view in the case of agency models, a responsibility of the platform operator can only be justified by the fact that it bears objectively all significant chances and risks of the transaction (ie, contractual partner from an economic point of view). In that case, the responsibility of the platform operator, again contrary to Article 18(1) of the Academic Draft, should not depend on whether the relevant circumstances are apparent to the customer ex ante. As far as agency models are concerned, it is accepted that the retailer's responsibility does not depend on whether its internal arrangements with the seller-consumer were visible to the buyer-consumer. In platform constellations, too, the individual customer often does not have a comprehensive insight into the relationship between the platform operator and the supplier. Thus, the platform operator's responsibility should not depend on the ex ante knowledge of the customer'.

bears all significant economic changes and risks of the transaction with consumers, by acting as their actual contractual counterparty.

As a result, in the actual early stage of the *collaborative economy* expansionism, it seems that the objective regulatory approach of the E-Commerce Directive in the field of liability could show the right way forward in order to design a comprehensive legislative framework. The application of the predominant influence criterion to liability issues, if not interpreted according to a subjective approach, could guarantee a reasonable and satisfying level of consumer protection without stifling innovation, far from the piecemeal case-by-case approach of the Court of Justice on the relationship between the E-Commerce Directive and offline sector regulations.

Conclusions.

The regulatory approach to govern market relationships in the context of the *collaborative economy* should be investigated further. However, emphasizing the technological element from a legal perspective represents the first step of a broader research aiming at studying how traditional contract law and consumer law instruments could change in a digitized and decentralized *sharing economy* context. The legal interactions between consumers and the platform and between suppliers and the platform should be seen as two autonomous contracts, that are different from the offline services contract (between consumers and providers) and should comply with requirements tailored to the specific needs of *collaborative economy* consumers. From this standpoint, the technological element determines the triangular market structure of the *collaborative economy* (consumers-platform; platform-providers; providers-consumers) and should be emphasized when exploring the consequences on the way of conceiving and regulating legal relationships. This is because the digital layer enables consumers to empower themselves and become prosumers, so regulating in-depth this aspect represents the only way to govern transactions carried out in a platform. In doing so, except for mere intermediary and advertising platforms, collaborative platforms should be compared with providers of information society services, in such a way that consumers could be protected homogeneously. This does not mean that sector regulations for services offered through online platforms are irrelevant, but simply that they have a subordinate role, aiming at regulating specific (and fundamental) aspects concerning offline performance. On the contrary, the E-Commerce Directive is the minimum instrument that could ensure legal certainty without discriminations and difficult case-by-case assessments. Indeed, collaborative platforms are in the best position to ensure transparency requirements and principles governing online contracts, at least in their relationships with consumers and providers and, depending on the level of influence exerted, also in the internal agreements between consumers and suppliers.

The question of the allocation of liabilities is closely linked to the issue of the legal qualification of collaborative platforms. Indeed, the need to ensure legal certainty to consumers depends also in this field on the layer at which legal instruments should be conceived. To this end, a possible solution could be introducing a form of joint liability of platforms for non-performance of suppliers. Consumers should know for sure who is their actual counterparty liable in cases of non-performance, and, also from a practical perspective, active platforms have the legal structure and the required competence to manage complaints and compensation claims, and to correct mistakes or enforce suppliers to comply with supply requirements. The objective approach adopted by the E-Commerce Directive concerning safe harbor' provisions (art. 12-14) and the absence of a general obligation on platforms to monitor information and illegal activities (art. 15) could be applied to the *collaborative economy* with regard to the non-performance of underlying services in so far as platforms should not

be generally held liable for non-performance, but only if certain predetermined circumstances, related to the significant control (decisive influence) over offline services, occur.

Finally, the ELI Model Rules on Online Platforms represent the first comprehensive attempt to rationalize the legal issues raised by *peer-to-peer* marketplaces. However, the unclear coordination between transparency requirements and the criterion of predominant influence and the introduction of a form of reliance liability could undermine consumer law protections and merit further examination.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

The vulnerable business user: the asymmetric relationship between the business user and the platform

SILVIA MARTINELLI
Researcher Fellow at the University of Milan
Ph.D
Lawyer

Abstract

The Paper analyses the weakness of the business users in multimedia habitat and, in particular, in the platform economy. It underlines the vulnerabilities of business users, unprotected by consumer law and data protection, in a market characterized by strong dominant position, high network effects and high switching costs.

Firstly, it focuses on the governance and regulation power of the platform (and the weaker counter-part bargaining power of the business users) and on the prevision of the measures of suspension and termination of the services by the platform.

Secondly, the paper analyses ranking algorithms regulation and differentiated treatment with regard to the interest of business users.

Finally, it moves to data law and data access for analyzing article 9 of the Regulation 1150/2019 and suggests the introduction of further instruments to protect the business user and guarantee, at the same time, some improvement for competition.

Keywords: Business user - platform - asymmetries - contract - data - fairness - user - data portability - data access

Summary: 1. The vulnerable business user. – 2. The power of the platform: from the regulation to the suspension and termination of the services. – 3. Ranking algorithms and differentiated treatments. – 4. Data and business users: how to unlock business data?

1. The vulnerable business user.

In the analysis of the positions of vulnerability in social networks and multimedia habitats, we usually think about consumers, data subjects and minors. Nevertheless, we assist to the emersion of a new category of weaker user, the "business user", due to the lack of balance in the relationship with social networks and platforms, where the bargaining power of the business user is almost always very small[1].

The new "multi-lateral" digital services (i.e. Airbnb, Amazon, Uber) are characterized by high market concentration and the role of these platforms is to enable users' interactions and extract value from them. The expression "multi-sided market platform" is used to define the platforms that serve at least two distinct groups of users who need each other; the core

[1] European Commission, *Study on Contractual Relationships between Online Platforms and Their Professional Users* (2018); http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51624, accessed on 2.11.2020; G Smorto, 'La Tutela Del Contraente Debole Nella Platform Economy' (2018) 158 Giornale di diritto del lavoro e di relazioni industriali.

business of the platform is allowing the meeting and facilitating the interactions between the distinct groups. There are, therefore, at least two different groups of users, who are kept in contact by the platform, which creates the match thanks to data and algorithm and reduces information and transaction costs. Without the platform, these meetings would not have taken place (the platform is also called "catalyst"[2]) and for business users it becomes crucial in order to meet potential customers[3].

The business model of social network is based on the analysis of the data generated by the interaction between users to create, with data analysis and algorithms, the perfect match with another group of users, the advertisers (for example, Facebook). In the platform economy, the core interaction[4] is the transaction between a vendor/provider of a service and a customer (for example Amazon, Uber, Airbnb). In these cases, strong network effects which reduce competition and determine the affirmation of strong dominant positions can be observed[5]: a) for the "direct network effect" the value of joining the platform for the individual user increases with the number of users ("if all my friends are there, I want to be there"); b) for the "indirect network effect", more users on one side of the platform attract more users on the other side of the platform ("if my consumer/target is there, I want to sell/promote my products there"); c) for the "big data effect", or "big data advantage", the availability of a large amount of data increase the possibility to improve algorithms and create better matches[6]. The existence of strong direct and indirect network effects increases switching costs[7] and platform lock-in and creates and increases the current dominant positions. In a market characterized by few actors, it is crucial for the business users to be present in these platforms and their bargaining power decrease.

The business user is a "trader"[8] and he can be both a natural person or a legal person. The "trader user" usually is in a weaker position behalf the platform: as a customer, he cannot benefit from the European consumer protection; with regards to data, he is not always qualified as a data subject. The definition of personal data applies only to natural person and, therefore, it would apply only for traders who are a natural person[9].

The European Regulation 1150/2019 "on promoting fairness and transparency for

---

[2] D S Evans and others, 'Platform Economics: Essays on Multi-Sided Businesses' [2011] Competition Policy International 459.

[3] Regulation 1150/2019, whereas 2; European Commission (n 1).

[4] G G Parker, Marshall W Van Alstyne and S P Choudary, *Platform Revolution. How Networked Markets Are Transforming the Economy and How to Make Them Work for You* (W W Nothon & Company 2016); Sangeet Paul Choudary, *Platform Scale* (Platform Thinking Labs 2015).

[5] K A Bamberger and O Lobel, 'Platform Market Power' (2017) 32 Berkeley Technology Law Journal 1051; Evans and others (n 2); M E Stucker and A P Grunes, *Big Data and Competition Policy* (Oxford University Press 2016); J S Frank, 'Competition Concerns in Multi-Sided Markets in Mobile Communication' in R Podszun and others (eds), *Competition on the Internet* (Springer 2014); OECD, 'Rethinking Antitrust Tools for Multi-Sided Platforms' 228 <www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.htm>, accessed on 2.11.2020; D Mandrescu, 'Applying EU Competition Law to Online Platforms: The Road Ahead - Part 1' (2017) 38 Eclr 353; M Katz and J Sallet, 'Multisided Platforms and Antitrust Enforcement' (2018) 127 Yale Law Journal 2142.

[6] M E Stucker and A P Grunes (n 5); European Commission, 'Enter the Data Economy' [2017] EPSC Strategic Notes 1 <https://ec.europa.eu/epsc/publications/strategic-notes/enter-data-economy_en>, accessed on 2.11.2020.

[7] "Switching costs" are the barrier costs that users may face when seeking to switch to another platform and they increase if there are some network effects.

[8] Directive 83/2011, art. 2, para 1, n. 2.

[9] S Martinelli, 'Commento All'art. 4 Del GDPR (Definizioni)' in A Barba and S Pagliantini (eds), *Commentario del Codice Civile (diretto da E. Gabrielli)* (Utet 2019).

business users of online intermediation services"[10] define the business users as "any private individual acting in a commercial or professional capacity who, or any legal person which, through online intermediation services offers goods or services to consumers for purposes relating to its trade, business, craft or profession"[11]. The new definition is introduced in order to determine the scope of the Regulation, whose aim is the promotion of "fairness and transparency for business users of online intermediation services". Hence, the Regulation applies only to traders on the offer-side.

The vulnerability of the business user occurs both on the demand side and on the supply side. However, the issue is more persistent on the supply side, since the platform is always designed for the benefit of the final customer, the user on the demand side[12].

The platform economy, also called "gig economy", enables new forms and possibilities to offer goods and services: "everyone can be employer of themselves". At the same time, individuals with no contractual power and without experience and knowledge of the sector often start an activity and assume the relative risks, without social protection and with different degrees of real autonomy.

The Regulation 1150/2019 introduces new rules for online intermediaries and search engines which offer services to users established in the Union. These measures are related to: conclusion of the contract and unilateral changes, measures for the suspension and termination of the service, ranking and transparency on the parameters, different treatment between users and access to data. In addition, the Regulation requires the implementation of an internal complaints management system, introduces mediation and the possibility, for organizations and associations that have a legitimate interest, to take action before competent national courts in the Union "to stop or prohibit any non-compliance by providers of online intermediation services or by providers of online search engines, with the relevant requirements laid down in this Regulation"[13].

This legislative instrument can only be a first step. In particular, access to data, suspension/ limitation measures and the use of algorithms and ranking systems require further analysis efforts and the development of tools to protect business users in respect of big platforms and the market.

2. The power of the platform: from the regulation to the suspension and termination of the services.

All activities and interactions between users which take place in the platform are subject to the contractual regulation unilaterally provided by the provider of the platform. The contractual regulation creates a "closed environment"[14] where users enter into a relationship through the communication possibilities technically offered by the platform and subject to the rules that it provides in the exercise of its private autonomy.

The platform builds this environment, chooses the rules, monitors their compliance, decides the application of sanctions in case of violation and executes the decisions. The whole technical structure of the platform (software, data and algorithms), the rules that regulate it and the control it carries out, together with its users and their data, establish the

[10] C Cauffman, 'New EU Rules on Business-to-Consumer and Platform-to-Business Relationships' (2019) 26 Maastricht Journal of European and Comparative Law 469; A Palmieri, *Profili Giuridici Delle Piattaforme Digitali* (Giappichelli 2019); C Twigg-Flesner, 'The EU's Proposals for Regulating B2B Relationships on Online Platforms – Transparency, Fairness and Beyond' (2018) 7 European Consumer and Market Law 222.
[11] Regulation 1150/2019, art. 2, para 1, n. 2.
[12] G G Parker, M Van Alstyne and S P Choudary (n 4).
[13] Regulation 1150/2019, art. 14, para. 1.
[14] T Rodriguez de las Heras Ballell, 'The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU' (2017) 3 The Italian Law Journal 8.

nature of the platform. Those elements are able to distinguish one platform from the others, to determine success or failure, and to constitute the service it offers. These aspects make the platform attractive and efficient. It plays not only an organizational role, but also a role of governance of the entire ecosystem.

The measures of suspension, termination or limitation of the services are the main sanctions applied by the platform. They apply to all types of users and they sanction contractual breaches. These breaches can be referred also to the violation of the "community rules", settled out for regulating the relationships between the users, or to the failure or incorrect provision of service of the supplier-user to provide the service to the customer-user. The provision of the service offered by the supplier is evaluated by customers using reputational feedback system and the problems occurring in the provision can be signaled to the platform using the "claim" system. Restrictions on the possibility to use the services provided by the platform are applied in case of a high number of "claim" unsolved or of low scores on the reputational feedback system. Furthermore, the platform has the possibility to sanction the supplier-user for a variety of conducts with different kinds of limitation: for example, Amazon, in case of delays in the delivery of the products, allows the sale only by relying on the shipping service provided by Amazon itself.

The lack of transparency in these sanctioning systems and the importance of the platform for the supplier-user generate an opaque system that can lead to abuse. The European Legislator has introduced article 16 of the Directive 770/2019 for consumers and article 4 (and part of article 3) of the Regulation 1150/2019 for the business user.

The Regulation establishes that providers of online intermediation services shall ensure that their terms and conditions "set out the grounds for decisions to suspend or terminate or impose any other kind of restriction upon, in whole or in part, the provision of their online intermediation services to business users"[15]. Furthermore, where a provider of online intermediation services "decides to restrict or suspend the provision of its online intermediation services to a given business user in relation to individual goods or services offered by that business user, it shall provide the business user concerned, prior to or at the time of the restriction or suspension taking effect, with a statement of reasons for that decision on a durable medium"[16].

The statement of reason shall contain "a reference to the specific facts or circumstances, including contents of third party notifications, that led to the decision of the provider of online intermediation services, as well as a reference to the applicable grounds for that decision referred to in point (c) of Article 3(1)". This is not necessary where the platform is subject to "a legal or regulatory obligation not to provide the specific facts or circumstances or the reference to the applicable ground or grounds, or where a provider of online intermediation services can demonstrate that the business user concerned has repeatedly infringed the applicable terms and conditions, resulting in termination of the provision of the whole of the online intermediation services in question"[17].

For terminations concerning the whole service offered by the platform, the communication must be at least 30 days before the measure takes effect[18]. The notice period shall not apply where a provider of online intermediation services: "a) is subject to a legal or regulatory obligation which requires it to terminate the provision of the whole of its online intermediation services to a given business user in a manner which does not allow it to respect that notice period; or b) exercises a right of termination under an imperative reason

[15] Regulation 1150/2019, art. 3, para 1, lett. c.
[16] Regulation 1150/2019, art. 4, para 1.
[17] Regulation 1150/2019, art. 4, para 5.
[18] Regulation 1150/2019, art. 4, para 2.

pursuant to national law which is in compliance with Union law; c) can demonstrate that the business user concerned has repeatedly infringed the applicable terms and conditions, resulting in the termination of the provision of the whole of the online intermediation services in question"[19].

In all cases (suspension, termination or restriction), the business user must have the "opportunity to clarify the facts and circumstances in the framework of the internal complaint-handling process" and, if the measure is revoked, the platform shall "reinstate the business user without undue delay, including providing the business user with any access to personal or other data, or both, that resulted from its use of the relevant online intermediation services prior to the restriction, suspension or termination having taken effect"[20].

The sanctioning powers of the platform constitute a very delicate aspect also in consideration of the strong dominant positions existing in the market, which can make the consequences of exclusion more prejudicial.

A greater *ex ante* transparency in contractual conditions and a clearest and fair procedure for the application of these measures, together with written and detailed communications for the exercise of the right of defense and appeal, are crucial. The Regulation moves in this direction, but could be further detailed, also through the adoption of *soft law* tools or technical standards, such as ISO standards, as is happening with regard to *reputational feedback systems*[21].

The new Digital Services Act package[22], announced by the European Commission, aims also to introduce new measures on notice and take down mechanism (used for the removal of illegal content online), but it does not take into account suspension and termination measures. The IMCO Committee calls the Commission to require platforms to verify the information and identity of the business partners and to strengthen information requirements for business customers, but neither further protection of business users on the supply-side seems to be on the plan. The drafted proposal contains also the introduction of an "ex ante regulation of systemic platforms" for the "online gatekeepers" of the digital economy; maybe, this could be the right context to introduce measures to protect all types of users.

3. Ranking algorithms and differentiated treatments.

Algorithms are the true heart of the platform: they determine the flow of the news on social networks and advertised products related to each and every action of the user. In the platform economy, the match between customers and suppliers is decided by the algorithm, and the functioning of this algorithm becomes crucial for the supplier who wants to sell on the platform. These aspects can also create competition-related issues: algorithms can distort competition and lead to unfair commercial practices. The choices on the information provided for customers can distort competition, can be considered inequal treatment of business users and constitute unfair commercial practices.

With regard to the use of algorithms for ranking of products and services, the European

[19] Regulation 1150/2019, art. 4, para 4.
[20] Regulation 1150/2019, art. 4, para 3.
[21] ISO 20488:2018, Online customer reviews. Principles and requirements for their collection, moderation and publication.
[22] Ursula von der Leyen, 'A Union That Strives for More. My Agenda for Europe' 24 <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf>, accessed on 2.11.2020; IMCO, 'Draft Report with Recommendations to the Commission on Digital Services Act: Improving the Functioning of the Single Market' [2020] (2020/2018(INL)).

Legislator introduced some protection for consumers with the Directive 2161/2019[23] and new measures for business users with article 5 of the Regulation 1150/2019, applicable to online intermediation services and search engines. Moreover, article 7 of the Regulation set out new rules regarding "differentiated treatment".

Article 5 of the Regulation establishes that providers of online intermediation services shall introduce in the terms and conditions information on "the main parameters determining ranking and the reasons for the relative importance of those main parameters as opposed to other parameters"[24] and that the provider of a search engine shall set out on the website "the main parameters, which individually or collectively are most significant in determining ranking and the relative importance of those main parameters, by providing an easily and publicly available description, drafted in plain and intelligible language, on the online search engines of those providers"[25].

The description shall be "sufficient to enable the business users or corporate website users to obtain an adequate understanding of whether, and if so how and to what extent" the ranking mechanism takes into account characteristics of goods and services, the relevance of those characteristics for those consumers and (only for search engines) the design characteristics of the website used by corporate website users[26]. The transparency requirement does not include the disclosure of the algorithm and the provider can omit "information that, with reasonable certainty, would result in the enabling of deception of consumers or consumer harm through the manipulation of search results"[27].

Search engines must also indicate where "the main parameters include the possibility to influence ranking against any direct or indirect remuneration paid by business users or corporate website users" and give "a description of those possibilities and of the effects of such remuneration on ranking"[28]. Furthermore, they must notify any alteration of the ranking order or delisting adopted for specific cases, offering to the business user the possibility to inspect the contents of the notification[29].

In addition, article 7 establishes that providers of online intermediation services shall describe, in their term and conditions, "any differentiated treatment which they give, or might give, in relation to goods or services offered to consumers through those online intermediation services" and indicate "the main economic, commercial or legal considerations for such differentiated treatment"[30]. Similarly, online search engines must indicate any differentiated treatments on the website[31]. In particular, the description should cover differentiated treatments on ranking, access to data, remuneration, additional tolls and services.

Ranking poses the widest and most widespread problems concerning the use of algorithms in terms of lack of transparency (the so-called "black box") and in terms of control mechanisms. The decision adopted by the algorithm can be evaluated in terms of

---

[23] In particular, the Directive 2161/2019, "amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules", introduce a new art. 6-bis in the Directive 83/2011 concerning marketplaces and, also, ranking parameters; modifies the Directive 29/2005, art. 7, adding two paragraphs, 4-*bis* and 6, concerning ranking and reputational feedback system.

[24] Regulation 1150/2019, art. 5, para 1.

[25] Regulation 1150/2019, art. 5, para 2.

[26] Regulation 1150/2019, art. 5, para 5.

[27] Regulation 1150/2019, art. 5, para 6.

[28] Regulation 1150/2019, art. 5, para 3.

[29] Regulation 1150/2019, art. 5, para 4.

[30] Regulation 1150/2019, art. 7, para 1.

[31] Regulation 1150/2019, art. 7, para 2.

lawfulness and unlawfulness with respect to multiple profiles. These include, in particular, those deriving from the principle of equality, formal and substantial, between citizens and from the protection of competition and the market. In the case of intermediation platforms, as well as in other fields of application, the introduction of the accountability principle and the risk analysis concerning the algorithmic activity[32] appear as the most suitable solutions to ensure flexible and substantial protection in an extremely technical context, in which the transparency of information, even where deemed possible in the presence of new forms of protection of the intellectual property of the algorithm, would not in itself be sufficient to protect the market and the subjects involved.

4. Data and business users: how to unlock business data?

In the multimedia habitat, data play a crucial role. In the platform economy, they are relevant for the matches, description of products and services, profiling of *customers*, *ranking* and *reputational feedback system*. Where they fall within the definition of "personal data"[33], the Regulation 679/2016, "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", will apply for the protection of personal data of natural persons and the free movement of data. However, data are relevant even beyond the GDPR, even the "non-personal data" and, in particular, the data related to the activities of the business users (products, clients, etc.) are essential for the business and the independence of the business user[34]. In particular, relevant data for business users comprehend: information on products and services, user identification details, data on individual transactions, business performance (i.e. information on all transactions taking place through the platform, customer behavior, analyses of market trends/developments)[35], business reputation.

The platform economy is a clear instance of the contrast between the opposing needs of data circulation, as "new oil", and the protection of privacy. In the platform economy, however, data circulation become more urgent to reduce lock-in effects and encourage competition in a highly centralized market. For example, the business user cannot import to a new platform the product description created on the platform, the data relating to customers, their purchasing preferences and the reputation acquired through the reputational feedback systems.

Users who are not natural persons are basically excluded from the benefits arising from the application of the General Data Protection Regulation. The concept of "person" referred in the Directive 46/95/CE "on the protection of individuals with regard to the processing of personal data and on the free movement of such data", repealed by the GDPR, had initially been transposed by the Italian legislator as encompassing legal entities, bodies and associations[36], thus determining an extension of the scope of the regulation also to legal

---

[32] A Koene and others, 'A Governance Framework for Algorithmic Accountability and Transparency' [2019] EPRS 1 <http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf>, accessed on 2.11.2020.

[33] Silvia Martinelli (n 9).

[34] P Hausemer and L Rabuel, 'Study on Data in Platform-to-Business Relations' [2017] European Commission; I Graef, S Y Wahyuningtyas and P Valcke, 'Assessing Data Access Issues in Online Platforms' (2015) 39 Telecommunications Policy 375 <http://dx.doi.org/10.1016/j.telpol.2014.12.001>; I Graef, J Verschakelen and P Valcke, 'Putting the Right to Data Portability into a Competition Law Perspective' [2013] The Journal of the Higher School of Economics, Annual Review 1; Silvia Martinelli, 'Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and "Porting Rights"' in L Reins (ed), *Regulating New Technologies in Uncertain Times* (Springer 2019).

[35] P Hausemer and L Rabuel (n 34).

[36] Art. 1, lett. c), l. no. 675/1996.

persons. With the dl n. 201/2011, converted with Law 214/2011, art. 40, the Legislator eliminated this reference, thus limiting the scope of application to natural persons. Thus, a part of business users cannot exercise the rights of the data subject.

The extension to legal persons, however, applies with reference to Directive 58/2002, relating to the processing of personal data and the protection of privacy in the electronic communications sector, the so-called "E-privacy Directive", also implemented in the Code for the protection of personal data, in Title X, dedicated to «Electronic communications». With reference to this Directive, the extension to natural persons, found in the definition of "abbonato"[37], reconfirmed by the Garante per la protezione dei dati personali with the Provvedimento no. 262 of 20.9.2012[38], where the Italian Data Protection Authority stated that, despite the aforementioned legislative intervention aimed at excluding the application to legal persons, the protection of legal persons should not be considered excluded and the concept of personal data should be considered, for the scope of the Directive 58/2002, as also extended to them. In particular, the Italian Authority argued that the concept of "personal data" should, in this case, be interpreted in connection to the notion of "abbonato" or "contraente", applicable to both natural and legal persons. Also with regard to the E-privacy Directive, the European Commission had proposed a revision, with a transition from Directive to Regulation, for adapting and coordinating the old rules with the GDPR. But this revision process has not still led to adoption of a definitive text[39]. With the entry into force of the GDPR, while pending the revision of the E-privacy regulation, the applicability of Directive 58/2002 to legal persons remains, due to the use of the term "subscriber". The current proposal for the E-privacy Directive proposed an analogous extension of the protection to legal persons, expressly mentioning them as well as referring generically to the "end user", but also in this text remains, at present, with regard to definition of "personal data", a mere reference to the GDPR[40].

Considering the weakness of business user platforms in this context, the possibility to extend the definition also for the use of online intermediation services or search engine should be evaluated. The relevant rights for business users are the right to access (now introduced also for business users by the Regulation 1150/2019) and right to data portability. Otherwise, the introduction of new forms of contractual protection of the business users regarding data, with mandatory rules, shall be considered.

With regard to the right to data portability, the GDPR provides the data subject both the right to receive a copy (in a structured format, commonly used and readable by an automatic device), and the right to transmit such data to another data controller. This could help the competition in the market; however, it is the worst-implemented right of the GDPR and a real use of this instrument is still to come.

Also the Digital Content Directive, protecting consumers "on certain aspects concerning contracts for the supply of digital content and digital services", has introduced some first regulation on the destiny of the data at the end of the contractual relationship. Article 16 of the Directive 770/2019 ("Obligations of the trader in the event of termination") establishes that the trader shall "refrain from using any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied

[37] Art. 4, 2° co., lett. c) of D.lgs. 196/2003.

[38] Provvedimento n. 626, 20.9.2012, "in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011", doc. web n. 2094932.

[39] "Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", COM/2017/010 final - 2017/03.

[40] Recital 3 of the Proposal.

by the trader, except where such content: (a) has no utility outside the context of the digital content or digital service supplied by the trader; (b) only relates to the consumer's activity when using the digital content or digital service supplied by the trader; (c) has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts; or (d) has been generated jointly by the consumer and others, and other consumers are able to continue to make use of the content"[41]. And, most of all, except in the referred cases (a), (b) and (c), the trader "shall, at the request of the consumer, make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader" (free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format) [42].

At the moment, with regards to data and business users, only article 9 of the Regulation 1150/2019 ("Access to data") applies. The provider of online intermediation services shall include in its terms and conditions "a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services"[43]. The description must inform the business user about: a) the possibility for the platform to access personal and non-personal data provided or generated by consumers and business users for the use of the services, specifying the categories of data concerned and conditions; b) the possibility for the business user to access the same data, specifying the categories and conditions; c) the possibility of accessing such data in aggregate form ("provided by or generated through the provision of the online intermediation services to all of the business users and consumers"), with specification; d) the provisions to third parties of the data and, "where the provision of such data to third parties is not necessary for the proper functioning of the online intermediation services, information specifying the purpose of such data sharing, as well as possibilities for business users to opt out from that data sharing"[44].

Both provisions, art. 16 of the Directive and art. 9 of the Regulation, provide detailed disciplines of terms and conditions in relation to the data: the first with regard to the time of the end of the relationship, the second with respect to the data processed and to which it is possible to access or to which the platform or third parties can access.

It is not clear why, in this case too, it should not be possible to adopt a uniform discipline that encompasses both disciplines, since even if the consumer also enjoys the rights set out in Regulation 679/2016, these do not apply to non-personal data and he would remain, however, excluded from protection the *customer* who is not a consumer. The need for greater clarity and transparency with respect to the data processed and the "data cycle" is strongly felt for all users, also business users, now locked in the platform.

In conclusion, with regard to the business user, any regulation on the termination of contract is lacking, and no data portability right is provided. Article 9 elaborates a good distinction between the types of data processed and highlights the needs of business users with respect to the data; however, it settled-out mere information obligations.

The information obligations and the knowledge regarding the data processed may constitute a first step towards a negotiation, but the contractual weakness of the business user towards the platform makes it difficult to realize. New studies, policies and also legislative instruments introducing mandatory rules concerning data sharing should be

[41] Directive 770/2019, art. 16, para 3.
[42] Directive 770/2019, art. 16, para 3.
[43] Regulation 1150/2019, art. 9, para 1.
[44] Regulation 1150/2019, art. 9, para 2.

implemented to protect business users and the market.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

The omnibus directive and online price personalization: a mere duty to inform?

SEBASTIÃO BARROS VALE
LL.M in EU law at the College of Europe in Bruges (Belgium)
Lawyer in Portugal

Abstract

As part of the EU's New Deal for Consumers, Directive (EU) 2019/2161 (the Omnibus Directive) enshrines into European law a duty for traders to inform consumers who visit their online stores if the prices they are offered have been tailored based on their personal traits by a pricing algorithm. Although this commercial tactic sounds innovative, the phenomenon of Online Price Personalization (OPP) is not new, as retailers have been reported to embark on such practices since the turn of the millennium. Consumers have expressed feelings of discomfort and outrage towards OPP, even in cases where it could work to their advantage (i.e., leading them to pay a lower price when compared to other consumers). This paper will look to offer a clear definition of OPP, setting it apart from similar practices. It will also elaborate on how consumers should be informed about OPP under the Omnibus Directive and seek to outline the current constraints EU law poses to OPP. While EU anti-discrimination law is briefly analyzed, deeper focus will be dedicated to Privacy & Data Protection Law and the Unfair Commercial Practices Directive (UCPD) as means to protect consumers from OPP, regardless of whether it discriminates against them or not. The paper will try to demonstrate how, in several cases, traders deploying OPP may be misleading consumers for the purposes of Articles 6 and 7 of the UCPD, and how the "average consumer" criterion is unfit to legally assess the fairness of OPP under the UCPD.

Keywords: Online Price Personalization - European Union - New Deal for Consumers - Discrimination - Omnibus Directive - General Data Protection Regulation - Unfair Commercial Practices.

Summary: Introduction – 1. Defining Online Price Personalization (OPP). – 2. The Omnibus Directive: an insufficient shield against OPP. – 3. The EU anti-discrimination framework: limited safeguards and a heavy burden of proof. – 4. EU Privacy and Data Protection law: a big hurdle for OPP. – 5. OPP as an Unfair Commercial Practice? – Conclusions.

List of Abbreviations:

AI = Artificial Intelligence
BEUC = The European Consumer Organization
Council = Council of the European Union
Charter = Charter of Fundamental Rights of the European Union [2000] O.J. C364 1
CJEU = Court of Justice of the European Union
CRD = Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (Consumer Rights Directive) [2011] OJ L304/64
DPA = Data Protection Authority, as per Article 4(21) GDPR

DPD = Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L281

EC = European Commission

EP = European Parliament

EDPB = European Data Protection Board created under Article 68 of the GDPR

ePrivacy Directive = Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2002] OJ L201

EU = European Union

GDPR = Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing DPD (General Data Protection Regulation) [2016] OJ L119/1

GGSD = Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services (Gender Goods and Services Directive [2004] OJ L373/37

Geo-blocking Regulation = Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC [2018] OJ LI60/1

OECD = Organization for Economic Co-operation and Development

Omnibus Directive = Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7

OPP = online price personalization

RED = Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (Race Equality Directive) [2000] OJ L180

Rome I Regulation = Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations [2008] OJ L177/6

Services Directive = Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [2006] OJ L376/36

TEU = Consolidated Version of the Treaty on European Union [2008] OJ C115/13. Treaty on European Union (Maastricht Treaty) art G5

TFEU = Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326

UCPD = Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L149/22

WP29 = Working Party created under Article 29 of the DPD
WTP = willingness to pay

Introduction.

Imagine you are comparing dog food prices online, on the website where you normally buy it, and notice the retailer was offering a great deal for this normally expensive packet. Then, after logging in with your user credentials, the deal suddenly disappears, as the price for each such packet rises significantly. Does this make you think that you are being asked to pay more because of who you are? You could be, as you were probably subjected to Online Price Personalization (OPP).

Is this practice lawful, since it (at least) seems to make consumers uncomfortable?[1]

As this article will try to demonstrate, the example above amounts to one of the simplest and less intrusive currently used forms of OPP, based on a consumer's purchase history in said trader's website. In fact, it is safe to assume (and, arguably, not too shocking for consumers) that traders retain information about their customers' past purchases, notably for accounting and tax purposes. What may feel unacceptable for consumers is to be served with a higher price for the same goods than their next-door neighbor, just because the trader uses said information to calculate his/her willingness to pay (WTP) a premium over the normal price.[2] On the other hand, the idea that consumers are more suspicious of data-intensive forms of OPP and that they are more willing to accept OPP if it works to their advantage (ie leading to price reductions) is under debate and needs further study.[3]

What if the information used by a certain trader to adjust the price which is shown to you would not be limited to what you had purchased from that trader before? What if the price "tag" would be calculated by checking these purchases against the location of the device you have been using to access the website over the last 6 months and the websites you visited that week? What if the trader, from that information, infers – accurately or not – that you live in a distant EU country, are experiencing financial trouble, belong to an ethnic minority

[1] In a 2005 survey conducted by Turow, "87% of respondents thought that it was wrong to charge different people different prices online for the same product during the same hour [and] 84% thought that websites ought to inform customers if they engaged in discriminatory pricing", as noted by A A Miller in 'What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing' (2014) Journal of Technology Law and Policy Vol. 19, 87. See J Turow & L Feldman, 'Open to Exploitation: America's Shoppers Online and Offline' (2005), Annenberg School of Communications, 6–12. In another study conducted by Turow and others, 78% of the respondents did not want "discounts (…) tailored for you based on following (…) what you did on other websites you have visited". See J Turow and others, 'Americans Reject Tailored Advertising and Three Activities that Enable it' (2009), available at http://ssrn.com/abstract=1478214, consulted on 28th May 2020.

[2] As noted by EU officials, "if a consumer finds out after having made a purchase that the price paid was higher than what other consumers paid, personalised pricing may have a negative impact on the reputation of the seller which may result in lost revenue". See OECD (Directorate for Financial and Enterprise Affairs Competition Committee), *Personalised Pricing in the Digital Era – Note by the European Union* [2018], 6.

[3] Some scholars argue that not only when consumers are economically disadvantaged by OPP do they feel unease with such practices. To quote Priester, Robbert and Roth, "In the face of similar transactions, an experienced price difference leads to the feeling of inequality and negative fairness perceptions" from the consumer. "A judgment of unfairness is generally associated with negative feelings such as unease or guilt when the inequality is to the buyer's advantage". See A Priester, T Robbert & S Roth, 'A special price just for you: effects of personalized dynamic pricing on consumer fairness perceptions' (2020) Journal of Revenue and Pricing Management 19, 99–112, 104 and 105. Zuiderveen Borgesius & Poort also argue that "The mere fear or suspicion of paying a premium could cause people to dislike personalized pricing". See F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) Journal of Consumer Policy 40, 347–366, 355.

or that you are gay and, for one or more of those reasons, decides to increase the prices you see? Would it make it better if the trader used those types of information to decrease your price, instead?

Despite ethical concerns raised by OPP and the public and media scrutiny[4] every time OPP practices are revealed, there are not many rules directly addressing OPP in EU law. In fact, legal scholars tend to claim that under the existing framework, OPP per se is not unlawful, unless – and only to the extent that – it incidentally breaches rules relating to competition, anti-discrimination, data protection or consumer law.[5]

Although reports of OPP have surfaced since the beginning of the 21st-century[6], and that OPP's effects on consumer welfare have been called into question[7], only in late 2019 did the EU legislator specifically address the issue, with a view to reducing the information asymmetry[8] between traders deploying OPP techniques and the targeted consumers. But is merely forcing traders to inform consumers about the use of OPP enough to protect them from unfair practices in this regard?

This paper will try to outline how the newly enacted Omnibus Directive, as well as other existing EU law instruments, may be leveraged to shield consumers[9] against these controversial practices. It is divided into 5 parts: the first (I) is devoted to defining OPP – distinguishing it from other close phenomena – and pricing algorithms; the second (II) will look into the transparency requirement stemming from the Omnibus Directive and the worries that remain; the third (III) will briefly point out whether and how EU anti-discrimination laws are up to the task; the fourth (IV) shall argue that EU privacy and data protection law may pose serious hurdles to merchants who deem to use pricing algorithms; and the fifth (V) will explore how OPP may constitute, in some cases, unfair commercial practices, forbidden under the UCPD.

Due to time limitations, the paper will not dive into the implications of EU competition law to OPP. Some authors, however, argue that constrains to OPP from this field of law are unlikely to arise if the trader deploying it does not have a dominant position in its market and abuses said position – under Article 102 of the Treaty on the Functioning of the

---

[4] See, as examples, Harvard Business Review, *How Retailers Use Personalized Prices to Test What You're Willing to Pay*, 20th October 2017, available at https://hbr.org/2017/10/how-retailers-use-personalized-prices-to-test-what-youre-willing-to-pay, consulted on 26th May 2020; and Time, *Orbitz Shows Higher Prices to Mac Users*, 26th June 2012, available at https://business.time.com/2012/06/26/orbitz-shows-higher-prices-to-mac-users/, consulted on 26th May 2020.

[5] For further notes on the lawfulness of OPP, see F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3); L Drechsler & J C Benito Sánchez, 'The Price Is (Not) Right: Data Protection and Discrimination in the Age of Pricing Algorithms' (2018) European Journal of Law and Technology 9(3); J A Gerlick & S M Liozu, 'Ethical and legal considerations of artificial intelligence and algorithmic decision-making in personalized pricing' (2020) Journal of Revenue and Pricing Management 19, 85–98; and A M Sears, 'The Limits of Online Price Discrimination in Europe' (2020) The Columbia Science & Technology Law Review Vol. XXI.

[6] The first notable OPP "scandal" was the Amazon 2000 initiative to offer online shoppers prices tailored to their unique characteristics, which ended up with the company refunding its outraged customers. See P Krugman, Reckonings; What Price Fairness?, The New York Times, 4th October 2000, available at https://www.nytimes.com/2000/10/04/opinion/reckonings-what-price-fairness.html, consulted on 1st June 2020.

[7] See OECD, *Personalised Pricing* (n 2), 5.

[8] According to Zuiderveen Borgesius & Poort, "Transparency about which companies engage in price personalization could mitigate this information asymmetry: Consumers may choose online shops that do not personalize prices". See F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), 359.

[9] We will focus on consumer OPP only, and not OPP affecting customers making purchases or shopping around online for purposes included in their trade, business, craft or profession. See Article 2(1) of the CRD.

European Union –, which may be challenging to prove in a given case of OPP.[10]

I will neither address OPP from economical, sociological nor psychological points of view, although these may be occasionally brought to the discussion to beef up certain legal arguments.

1. Defining Online Price Personalization (OPP).

For the purposes of this paper, OPP shall be defined as the possibility of offering different prices to specific consumers for the same product, equal to each consumer's presumed maximum willingness to pay (WTP) for that product, which are automatically calculated and presented to consumers by a pricing algorithm.

In turn, a price algorithm shall mean a well-defined computational procedure that takes some value, or set of values, as input to determine price as an output for a particular consumer. These "values" are, normally, consumers' unique characteristics (eg. "iPhone user", "IP address from Orahovica, Croatia", "visited diageo.com twice in the last 24 hours") – or labels/profiles based on such characteristics (eg. "Wealthy Mother", "Remote location", "Occasional Drinker") which inform the decision taken by the pricing algorithm. More complex pricing algorithms may consider additional factors other than the consumer's WTP, such as the cost of delivering goods or services to the consumer's location or the likelihood that a specific consumer (eg. given his/her putative age, credulity or need) will become a long-time customer.

Although some authors argue that pricing algorithms are widely used across the internet[11], evidence shows otherwise.[12] Miller, more cautiously, claims that "because of the prevailing secrecy in the consumer data industry, it is a matter of conjecture how businesses actually translate the detailed profiles (…) into individual price offers, and how widespread these practices are."[13]

The author also delves into the data brokerage industry, making it clear that many online traders deploying pricing algorithms rely on third party-built customer profiles to target consumers with personalized prices. These data brokers use a variety of tracking technologies (such as cookies, web beacons, pixels and device fingerprinting) to follow internet users' digital trail. By combining this wealth of data "with advanced data-mining techniques [it is possible to] discover associations and connections between demographic characteristics and preferences for products, or (…) [to] predict consumers' reactions to changes in price or special deals"[14].

Often, traders will count on those or other (such as data analytics) companies'

---

[10] See Sears, 'The Limits of' (n 5), 8-14, and I Graef, 'Algorithms and fairness: What role for competition law in targeting price discrimination towards end consumers?' (2018) Columbia Journal of European Law 24 (3), 542-554.

[11] Drechsler & Benito Sánchez argue that "Algorithms determining these prices are ubiquitous in the online environment, where merchants are able to process unprecedented amounts of personal data and generate complex profiles of consumers". See Laura Drechsler & Benito Sánchez, 'The Price is (Not) Right' (n 5), 1.

[12] See OECD, *Personalised Pricing* (n 2), 7: "personalised pricing does not seem to be present in the EU on any significant scale, at least for the moment". See also Ipsos, London Economics & Deloitte, *Report for DG JUST "Consumer market study on online market segmentation through personalised pricing/offers in the European Union"* [2018], available at https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf, consulted on 1st June 2020, 260 and 261.

[13] Miller, 'What Do We Worry' (n 1), 51 and 52.

[14] ibid 49. See also Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 262: "e-commerce websites that want to personalise results do not always collect and subsequently process consumer data/profiles themselves; instead they often use specialised companies' personalisation or analytics software or services."

personalization software "for the optimization of their (…) pricing strategy" and to ensure each consumer is served with a personally tailored price when they visit their websites.[15] The incorporation of AI (namely, machine learning) in these pricing algorithms "for detecting patterns in data collected on consumers' purchasing history, product and pricing preferences (…) can be used for predictive recommendations, offers and prices."[16] Even if they may issue generic instructions to said companies about the way they deem to target their customers for OPP purposes, traders are frequently not aware of the details of the functioning of the pricing algorithms, notably of the types of data which are fed into them and of the logic involved in the automated pricing decision-making, as those are the suppliers' "closely guarded trade secrets."[17] As we shall see below, this may pose challenges to traders vis-à-vis their transparency legal obligations towards consumers relating to OPP.

Although many authors[18] use the term online price discrimination when referring to what we described above as OPP, it is important, to ensure that an unbiased view of the phenomenon of OPP is kept, to distinguish between both practices. Even if price discrimination practices also rely on the collection and analysis of data about potential or current customers to define a price for those specific customers, those differentiate between customers or groups of customers – for price tailoring purposes – based on very sensitive observed or inferred characteristics of those customers, specially protected under EU anti-discrimination law. These characteristics include customers' gender, race, nationality and place of residence[19]. The European Commission (EC) Guidance on the application of the UCPD also makes a similar distinction between both concepts, clarifying that "Price discrimination is where a trader applies different prices to different groups of consumers for the same goods or services"[20]. The Guidance then mentions some grounds based on which direct or indirect[21] discrimination is forbidden, such as the ones highlighted above.

---

[15] Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 262. On page 78, the report mentions several companies offering this type of services (such as HayStacks and Tajitsu).

[16] ibid 97.

[17] Miller, 'What Do We Worry' (n 1), 51. Wachter & Mittelstadt argue that that the definition of "trade secret" in Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive) is broad enough to include algorithms, customer profiles derived from said algorithms and forecasts about a customer's future life (i.e., derived and inferred data). See S Wachter & B Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Columbia Business Law Review Vol. 2019 Issue 2, 117-119.

[18] See F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), and Sears, 'The Limits of' (n 5). Sears also states (6) that "Others prefer the term "price differentiation" in order to avoid the negative connotation of "discrimination." This may be commendable, as there are economic arguments that price discrimination may increase the total welfare of consumers and sellers."

[19] See Chapter III below for an analysis of these forbidden grounds of discrimination under EU law. Also in line with this distinction, see the letter by the Ministerie van Justitie en Veiligheid, *Moties op het terrein van gegevensbeschermingof* [2020], available at https://t.co/6aISm1DUp2?amp=1, consulted on 3rd June 2020, 2.

[20] EC, *Staff Working Document SWD(2016) 163 final Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices* [2016], 133.

[21] According to Article 2(2) of the Race Equality Directive (RED), "direct discrimination" shall be taken to occur where one person is treated less favorably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin, while "indirect discrimination" shall be taken to occur where an apparently neutral provision, criterion or practice would put persons of a racial or ethnic origin at a particular disadvantage compared with other persons. Thus, when a pricing algorithm takes a consumer's ethnic origin into account when making a pricing decision, this would be considered direct discrimination under the RED, including when it infers a certain consumer has a certain ethnic origin based on other observable aspects (eg. where the consumer lives, on the basis of his location history between 23:00h and 07:00h of each day over the course of a given month – see Judgement of 16th July 2015, *CHEZ Razpredelenie Bulgaria*, C-83/14, EU:C:2015:480, paragraph 59, ruling on inferences about Roma origin because of place of living). In turn,

Also relevant for the purposes of this paper is the distinction between first-degree price discrimination and third-degree price discrimination. According to Miller, "A first-degree price discrimination strategy requires that the firm be able to uniquely identify each consumer. It also requires a lot of information about the consumer's tastes and highest willingness to pay in order to tailor a price to an individual consumer[22]. (…) Third-degree price discrimination strategies require that the seller be able to identify at least whether the consumer has the relevant group trait that is used for discrimination, but does not necessarily need to uniquely identify consumers"[23].

Considering the above definition of OPP, first-degree price discrimination practices deploying pricing algorithms should also be considered as OPP practices. However, the same cannot be said of third-degree price discrimination, as the trader is not, in those cases, capable of singling-out a specific consumer through a unique identifier (eg. a cookie ID). The EU has recently taken the view that "The effect of first-degree price discrimination on consumer welfare is more likely to be harmful than third-degree price discrimination, because the producer captures up [or intends to capture up] to the entire surplus for all consumers, leaving them with potentially no gains from trade."[24]

It is also appropriate to separate OPP from dynamic pricing practices. Following the EC's Guidance on the UCPD, the latter means "changing the [displayed] price for a product in a highly flexible and quick manner in response to market demands". An example of this practice could be offering different prices in the same website, for the same products, at different times of the same days or different days of the same week, by raising the price when demand is surging or when supply in scarce[25]. Even if it has been reported[26] that consumers sometimes confuse OPP with dynamic pricing, the latter practice does not seem to draw significant concerns from the EU legislator, as the new information requirement stemming from the Omnibus Directive (which is analyzed in Chapter II below) does not apply to

---

algorithmic decision-making having a disproportionate impact on consumers of a certain ethnic origin without an objective justification would be considered indirect discrimination. See also the concept of "discrimination by association" in some EU Member-States laws (such as Portugal's Law no. 93/2017, of 23rd August, in Article 3(1)(d)), generally defined as discrimination which occurs because of one's relationship or association with a person or group of persons with certain specially protected characteristics (such as race, ethnicity or nationality). For more on how discrimination by association is often forbidden under EU law and the related CJEU's case law, see Wachter S, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) Berkeley Technology Law Journal Vol. 35 No. 2 (Forthcoming), 31-46.

[22] Zuiderveen Borgesius & Poort argue that "First-degree price discrimination refers to a situation in which each consumer is charged an individual price equal to his or her maximum willingness to pay. For first-degree price discrimination, the seller needs precise information about the buyer's willingness to pay (the reservation price). (…) In practice, such an extreme form of price discrimination will never occur, as sellers cannot learn the buyer's exact reservation price". F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), 351. On a similar note, see OECD, *Personalised Pricing* (n 2), 3: ""Perfect" price discrimination would mean charging each person the price that reflects their exact personal maximum willingness to pay. This is also known as "first-degree" price discrimination. Perfect first-degree price discrimination is unlikely to occur in practice." There are strong arguments, however, to support the view that, for first-degree price discrimination to occur, a trader does not need to know with absolute certainty the targeted consumer's WTP, but merely to attempt to calculate this individual WTP, based on the information at its disposal about the targeted consumer.

[23] Miller, 'What Do We Worry' (n 1), 56 and 57.

[24] See OECD, *Personalised Pricing* (n 2), 5.

[25] See EC, *Staff Working Document* (n 20), 132. See also Priester, Robbert and Roth, 'A Special Price' (n 3), 99: [dynamic pricing] "entails price changes over time due to fluctuations in supply, demand, competition, or other factors. Prices thus vary depending on the time of purchase but are the same across consumers at a given time".

[26] See The Guardian, *How much…? The rise of dynamic and personalised pricing*, 20th November 2017, available at https://www.theguardian.com/global/2017/nov/20/dynamic-personalised-pricing, consulted on 26th May 2020.

dynamic pricing.[27]

Lastly, OPP should not be mistaken for personalized ranking, which may be defined as the technique of altering of the order in which available options are displayed to users in e-commerce websites to suit their perceived interests and preferences.[28] This practice also entails the processing of data about each visitor and may even "entail an element of personalised pricing if the options ranked highest are actually there to fit the person's maximum willingness to pay"[29]. As increasing evidence about the ubiquity of personalized ranking has been recently found[30], this has also been addressed by the EU legislator in Article 4(5) of the Omnibus Directive, which establishes an obligation for merchants to inform consumers about the main parameters determining [this] ranking.

Now that a definition of OPP has been provided, the ensuing Chapter will plunge into how the Omnibus Directive tackles OPP, how traders should go by informing consumers about the use of pricing algorithms and whether this transparency duty suffices to empower consumers to take informed decisions.

2. The Omnibus Directive: an insufficient shield against OPP.

As part of the New Deal for Consumers[31], which was announced in April 2018, the Commission published a Directive Proposal[32] to, among other objectives, update certain aspects of the CRD in relation to traders' information duties towards consumers. This Proposal eventually led to the adoption of the Omnibus Directive, on 27th November 2019, whose information requirements on OPP will be analyzed below.

The original text of the Proposal did not contain any reference to OPP. However, the EP proposed (in first reading) certain amendments to the Proposal in early 2019, notably suggesting the incorporation of an additional information requirement in Article 6 of the CRD, which would require the trader to inform the consumer about "whether and how algorithms or automated decision making were used, to present offers or determine prices, including personalised pricing techniques."[33] The wording of this requirement was then

---

[27] See Recital (45) of the Omnibus Directive. This does not mean, however, that certain dynamic pricing practices may not be considered as unfair commercial practices in certain circumstances, as pointed out by the EC: "A dynamic pricing practice where a trader raises the price for a product after a consumer has put it in his digital shopping cart could be considered a misleading action under Article 6(1)(d) UCPD." See EC, *Staff Working Document* (n 20), 133.

[28] See OECD, *Personalised Pricing* (n 2), 3.

[29] ibid. This practice is also known as "price steering". For further insights on the matter, see A Hannak and others, 'Measuring price discrimination and steering on ecommerce web sites' (2014) Proceedings of the 2014 Conference on Internet Measurement Conference, 305–318

[30] See Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 42 and 43.

[31] See EC, *Review of EU consumer law - New Deal for Consumers* [2018], available at https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en, consulted on 23rd May 2020.

[32] EC, *Proposal for a Directive of the European Parliament and of the Council amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules, COM(2018) 185 final* [2018].

[33] EP, *Report on the proposal for a directive of the European Parliament and of the Council amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules (COM(2018)0185 – C8-0143/2018 – 2018/0090(COD))* [2019]

tweaked by the Council, which also inserted Recital (45) into the text[34]. Both would make their way to the final version of the Omnibus Directive.

Article 4(4)(ii) of the Omnibus Directive obliges traders to inform consumers, "where applicable, that the price was personalised on the basis of automated decision-making". Recital (45) of the Directive adds that "Traders may personalise the price of their offers for specific consumers or specific categories of consumer based on automated decision-making and profiling of consumer behaviour allowing traders to assess the consumer's purchasing power. Consumers should therefore be clearly informed when the price presented to them is personalised on the basis of automated decision-making, so that they can take into account the potential risks in their purchasing decision."

This approach recognizes how difficult it is for consumers to spontaneously realize that OPP is actually happening[35], and is in line with the EU legislator's tendency to protect consumers via evermore extending information duties incumbent upon traders.[36] On this particular matter, even before the enactment of the Omnibus Directive, Zuiderveen Borgesius & Poort have argued that traders were already obliged to inform consumers about the processing of their personal data for OPP purposes under the applicable privacy and data protection laws[37], in a clear and specific fashion[38]. However, despite the fact that, for traders, this new information requirement may feel like an unnecessary repeated burden, the advantage – for consumers – of having a specific information duty regarding OPP in the CRD relates to the legally required salience of the information under Article 6(1) of the CRD. In this regard, although the way in which traders will, in practice, comply with this information duty (eg. on the placement of OPP warnings and the level of detail of the information provided) is still a matter of conjecture,[39], it is already possible to draw some predictions.

The EC has recently stressed that, for the purposes of Article 4(4)(ii) of the Omnibus Directive, "The information about personalisation should be provided every time a personalised price is offered"[40]. This may mean that an "OPP tag" should be provided next to the displayed price. There is a chance that the industry will develop certificates or labels

---

[34] The amendments proposed by the Council, on 29th March 2019, may be found at https://www.europarl.europa.eu/RegData/commissions/imco/lcag/2019/03-29/IMCO_LA(2019)003440_EN.pdf, consulted on 23rd May 2020.

[35] In many cases, consumers may assume that, by seeing different prices on the same websites in two different visits when using the same device, they are being subject to OPP, when traders may be only experimenting with dynamic pricing (according to the time of the day, eg.). Users are more likely to detect OPP when they visit the same web shop using two different devices at the same time. But, then again, not all consumers have two different devices with internet access at their disposal to test this and the average consumer is not expected to be so diligent.

[36] See also See also Recital (2) of Services Directive: "A free market which compels the Member States to eliminate restrictions on cross-border provision of services while at the same time increasing transparency and information for consumers would give consumers wider choice and better services at lower prices." Evidence suggests, however, that this approach has been failing EU consumers. In a 2011 EC Special Barometer, more than a third of consumer respondents declared he or she was poorly informed about their rights as consumers and only 2% of respondents answered correctly to a set of questions relating to cooling-off periods, guarantee validity rights and unfair commercial practices. See EC, *Special Eurobarometer 342 / Wave 73.2 & 73.3. – TNS Opinion & Social* [2011].

[37] Notably, under Article 5(3) of the ePrivacy Directive and Articles 13(2)(c) and 14(2)(c) of the GDPR.

[38] See F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), 359.

[39] As Member-States are only required to transpose the Omnibus Directive by 28th November 2021 and to start applying the new rules from 28th May 2022. See Article 7(1) of the Omnibus Directive.

[40] EC, Recommendations for a better presentation of information to consumers (updated) [2019], available at https://ec.europa.eu/info/sites/info/files/sr_information_presentation.pdf, consulted on 26th May 2020, 10, n 18.

to indicate to consumers that the price they are seeing online has been calculated by a pricing algorithm. Alternatively, the Commission may also publish a template for the display of this information, as it already did with the current set of requirements of Article 6(1) of the Consumer Rights Directive[41].

What seems clear is that, in line with the general requirements of the CRD, information about OPP should be displayed "in a way appropriate to the means of distance communication used in plain and intelligible language"[42]. Furthermore, as generally the trader deploying OPP shall enter into a distance contract with the consumer for the selling of goods or the provision of services, the former is required to "make the consumer aware in a clear and prominent manner, and directly before the consumer places his order, of the information provided for in points (a), (e), (o) and (p) of Article 6(1)."[43] As information relating to OPP relates to price (which, in turn, is mentioned in indent (e) of Article 6(1) CRD) and given the Omnibus Directive has inserted this new information requirement as indent (ea) to Article 6(1), it is safe to assume that also the foregoing type of information should be provided in such a clear and prominent manner, and right before the consumer clicks the 'buy' button[44].

Given that consumers have a limited attention span for information provided by a trader before placing their orders, as they tend to avoid information overload by focusing on the elements which they consider to be more important (including price)[45], legally mandating traders to provide information about OPP in a salient manner such as this could help consumers take more conscious decisions about whether or not to engage with merchants deploying pricing algorithms. The effects of OPP tags on consumer purchasing habits are yet to be seen, however, as there is a chance they will largely be ignored by motivated buyers. Still, due to this new information requirements, and since consumers are known to be skeptical about OPP (see note 1), law-abiding online traders may be discouraged to deploy or keep using pricing algorithms, fearing consumers would disengage upon acknowledging they may be targeted with different prices than other consumers based on their personal characteristics.

Furthermore, the dissemination of OPP tags in online marketplaces and shops would create an opportunity for third-party auditors, policymakers, consumer associations and regulators alike to assess how widespread OPP practices are, which could prove useful for designing advocacy, regulatory or enforcement strategies for or against them.

Despite the adoption of the Omnibus Directive, however, concerns about OPP remain. Notably, and as outlined above, the level of detail of the information that traders are required to provide via OPP tags is not thoroughly defined in the Omnibus Directive. In this respect, there are arguments for keeping these tags very simple, much like warning labels, without

---

41 See Annex I of EC, *DG Justice Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council* [2014].

42 Article 8(1) CRD.

43 Article 8(2) CRD. According to Recital (39) CRD, these information elements should "be displayed in the close vicinity of the confirmation requested for placing the order". The EC adds that "the terms 'prominent manner' and 'close vicinity' in Recital (39) suggest stronger requirements on presenting information compared to the general requirements under Article 6(1) and 8(1). The information should be presented in a way that the consumer can actually see and read it before placing the order without being obliged to navigate away from the page used to place the order." See EC, *Recommendations* (n 40), 32.

44 The EC has clarified that "Article 8(2) of the Directive would in practice apply at the moment in which the consumer is asked to verify the order in line with the eCommerce Directive, i.e. to check the contents of the shopping basket before clicking on the 'buy' button". See EC, *Recommendations* (n 40), 32.

45 See M Vieira Ramos, 'Psicologia e Direito do Consumo: a Proteção do Consumidor face aos Efeitos das Modernas Práticas Comerciais' (2019) Anuário do Nova Consumer Lab 2019, 335-492, 345 and 346.

any details regarding the functioning of the pricing algorithm, so as to not overwhelm consumers with information and ensure the tags' effectiveness. This, however, may be in contradiction with the traders' transparency duties under the GDPR regarding automated decision-making (as detailed in Chapter IV, below).

Moreover, in a December 2019 question to the EC – which may well reflect the public suspicion of OPP –, a Member of the EP observed that "AI can be used to engage in far-reaching individual online price discrimination (personalization of prices) based on consumer data such as location, purchasing history, surfing behavior, etc.", and queried whether the EC was aware of this type of practices and if it was "considering a general prohibition on online price discrimination"[46]. In his March 2020 answer, EC's Justice Commissioner Didier Reynders highlighted that practices such as online price discrimination, dynamic pricing and OPP are regulated under several EU law instruments, from the EU's anti-discrimination, privacy, data protection and consumer acquis. Therefore, even if such practices are not forbidden per se, the EC committed to monitoring "the prevalence of online price discrimination and, if necessary, [to] take further action to ensure a high level of consumer protection."[47],

Having that said, the article now elaborates on how the EU's anti-discrimination laws protect consumers against unjustified online price discrimination and, therefore, certain forms of OPP.

3. The EU anti-discrimination framework: limited safeguards and a heavy burden of proof.

The EU's primary law directly refers to non-discrimination on several provisions. Article 2 of the Treaty on the European Union states that "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail." Article 3 adds that the EU shall "combat social exclusion and discrimination", as well as promote "equality between women and men". Articles 10, 18, 19 of the Treaty on the Functioning of the European Union (TFEU) also refer to the EU's goal to combat discrimination, notably based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. Article 21 of the Charter of Fundamental Rights of the European Union (CFREU)[48] further prohibits discrimination "based on any ground such as sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation", as well as nationality.

In principle, EU primary law instruments such as the ones cited are only binding for EU institutions and their Member-States, and not for private parties.[49] The CJEU has, however,

---

[46] EP, Question for written answer E-004289/2019 to the Commission, by Kris Peeters (MEP), 9th December 2019, available at https://www.europarl.europa.eu/doceo/document/E-9-2019-004289_EN.html, consulted on 23rd May 2020.

[47] EC, *E-004289/2019 Answer given by Mr Reynders on behalf of the European Commission* [2020], available at https://www.europarl.europa.eu/doceo/document/E-9-2019-004289-ASW_EN.html, consulted on 23rd May 2020.

[48] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1.

[49] Article 51(1) of the CFREU states that "The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law." The CJEU has ruled that, for EU primary law to have horizontal direct effect (i.e., to bind private entities), it must create precise, clear and unconditional obligations for private entities,

pointed out the horizontal effect of certain primary EU law provisions, namely when a general principle of EU law – such as the principle of non-discrimination on grounds of age[50] or on grounds of religion or belief[51] – is at stake.

Despite the above considerations, traders deploying OPP will mostly look into other more densified EU legislative instruments – such as Regulations[52] and Decisions[53] - to understand what their obligations regarding OPP are. This is without prejudice to EU Member-State law transposing the EU's Directives[54], which is directly applicable to such players.[55]

The EU has passed some legislative instruments which, if duly enforced at Member-State level, may be liable to prevent traders from carrying out online price discrimination. The Race Equality Directive (RED), which applies to "all persons, as regards both the public and private sectors", prohibits the discrimination of individuals, when accessing goods or services, on grounds of their racial or ethnic origin[56]. However, even if, at first sight, this Directive seems like a viable tool for consumers who have been online targeted with a personalized price by reason of their observed or inferred ethnic or racial origin to seek compensation or other suitable remedies, Sears notes that "demonstrating that a person was discriminated against on the basis of race or ethnicity through online price discrimination may be quite difficult, in particular where algorithmic personalized pricing operates within a "black box"." Furthermore, if one considers that the plaintiff must also show "that the only reasonable explanation for the difference in treatment is [his/her] protected characteristic"[57] (under Article 8(1) of the Directive), then the RED ceases to look like such a bright avenue for consumers.

The same arguments are valid when we look at the protection awarded to consumers by the Gender Goods and Services Directive (GGSD)[58], with an additional nuisance related to

---

which do not call for additional measures. See Judgement of 5th February 1963, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration*, 26-62, ECLI:EU:C:1963:1.

[50] See Judgement of 19th January 2010, *Seda Küçükdeveci v Swedex GmbH & Co. KG*, C-555/07, ECLI:EU:C:2010:21, paragraphs 21 to 23.

[51] See Judgement of 17th April 2018, *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung eV*, C-414/16, ECLI:EU:C:2018:257, paragraph 76.

[52] See Article 288(2) TFEU.

[53] See Article 288(4) TFEU.

[54] See Article 288(3) TFEU.

[55] The CJEU has consistently denied conferring horizontal direct effect to Directives, even when their respective deadline for Member-State transposal had already elapsed (see, *inter alia*, Judgement of 26th February 1986, *Marshall v Southampton and South-west Hampshire Area Health Authority*, 152/84, ECLI:EU:C:1986:84, paragraph 48). However, in what is known as the principle of indirect effect (or *principe d'interprétation conforme*), national courts are bound to interpret their domestic laws in accordance with any Directives whose transposition period has elapsed, as far as possible. See Judgement of 10th April 1984, *Von Colson v Land Nordrhein Westphalen*, 14/83, ECLI:EU:C:1984:153, paragraph 28, and Judgement of 13th November 1990, *Marleasing SA v La Comercial Internacional de Alimentacion SA*, C-106/89, ECLI:EU:C:1990:395, paragraph 8. In some cases, the CJEU has awarded indirect effect to Directives whose transposition period had not yet elapsed, when general principles of EU (such as non-discrimination) were at stake. See note 146, below.

[56] Article 3(1)(h) of the Race Equality Directive. According to CJEU case law, this shall include the provision of healthcare services. See Judgement of 12th July, *B.S.M. Geraets-Smits v Stichting Ziekenfonds VGZ and H.T.M. Peerbooms v Stichting CZ Groep Zorgverzekeringen*, C-157/99, ECLI:EU:C:2001:404, paragraph 55.

[57] See Sears, 'The Limits of' (n 5), 31 and 33.

[58] The GGSD lays down a framework for combating discrimination based on sex in access to and supply of goods and services and applies to all persons who provide goods and services (Articles 1 and 3(1) GGSD). The CJEU has ruled that considering the gender of the insured individual as a risk factor in insurance contracts constitutes discrimination, thereby invalidating former Article 5(2) GGSD – which allowed for such discrimination. See Judgement of 1st March 2011, *Association Belge des Consommateurs Test-Achats ASBL and Others v. Conseil des ministres [GC]*, C-236/09, ECLI:EU:C:2011:100, paragraphs 30 to 33. See also Article 9(1) GGSD on the burden of proof.

the fact that national legislators and courts have transposed and interpreted the Directive with substantial differences[59] and, thus, not all EU jurisdictions grant the same level of protection to consumers against pricing algorithms which take a consumer's gender as a decisive factor.

As mentioned by Commissioner Reynders in his March 2020 letter (see note 47), Article 20(2) of the Services Directive also generally prohibits consumer discrimination on the basis of their nationality or place of residence when accessing services[60]. Aimed at bolstering cross-border trade[61], but arguably still applicable in intra-EU Member-State transactions between traders and consumers, this prohibition is without prejudice to the traders' possibility of invoking objective criteria for offering different prices to different consumers for the same products or services on the basis of each consumer's location (which may be obtained from the consumer's device GPS coordinates – if their use has been consented by the consumer[62] – or from the device's IP address). These criteria may be linked to "additional costs incurred because of the distance involved[63] or the technical characteristics of the provision of the service, or different market conditions, such as higher or lower demand influenced by seasonality, different vacation periods in the Member States and pricing by different competitors, or extra risks linked to rules differing from those of the Member State of establishment", or the lack of the required intellectual property rights in the territory where the goods should be delivered.[64]

It is noteworthy that, out of the 532 complaints received by the European Consumer Centres Network (ECC-Net) between January 2013 and December 2015 related to Article 20(2) Services Directive discrimination, 68% of them were connected with "price or service differentiation [in] the purchase of goods, such as electronic goods, household appliances, vehicles, clothes, books, music or data downloads."[65] ECC-Net's report further noted that consumers often struggle to identify and find the contact details of the adequate enforcement bodies.[66] Gathering relevant documentary evidence to support consumers' claims may be

---

[59] On this, see Sears, 'The Limits of' (n 5), 32.

[60] The CJEU has made clear that this prohibition extends to the activity of retail trade in goods. See Judgement of 30th January 2018, *College van Burgemeester en Wethouders van de Gemeente Amersfoort v. X BV (C-360/15), and Visser Vastgoed Beleggingen BV v. Raad van de Gemeente Appingedam (C-31/16)*, Joined Cases C-360/15 and C-31/16, ECLI:EU:C:2018:44, paragraph 97. In turn, the EC points to the concept of "service" under Article 57 TFEU and offers a non-exhaustive list of services covered by the Directive, including "distribution of goods and services (retail), services in the field of tourism such as travel agencies, leisure services (…), the organisation of events, advertising and recruitment services." See EC, *Staff Working Document SWD(2012) 146 final with a view to establishing guidance on the application of Article 20(2) of Directive 2006/123/EC on services in the internal market ('the Services Directive') Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the implementation of the Services Directive: A partnership for new growth in services 2012-2015* [2012], 9.

[61] See M Karlson Jernbäcker, 'Article 20 (2) of the Services Directive - A prohibition against consumer discrimination' (2014) Uppsala University.

[62] See Article 9(1) of the ePrivacy Directive.

[63] However, the EC has stated that failure to supply due to lack of delivery options, due to the contractual relationship between independent undertakings, or due to higher charges for cross-border payments (in euro) are unlikely to be accepted as objective reasons for offering higher prices to consumers. See EC, *DG Internal Market and Services IMCO Working Group on the Digital Single Market, Article 20(2) Services Directive* [2013], available at https://www.europarl.europa.eu/document/activities/cont/201303/20130314ATT63206/20130314ATT63206EN.pdf, consulted on 1st June 2020.

[64] See Recital (95) of the Services Directive.

[65] ECC-Net, *Do Invisible Borders Still Restrict Consumer Access to Services in the EU?* [2017], available at https://ec.europa.eu/internal_market/scoreboard/_docs/2017/european_consumer_centre_network/services-directive-report_en.pdf, consulted on 1st June 2020, 6.

[66] ibid 45.

particularly difficult in Article 20(2) Services Directive-related online price discrimination, as consumers would need to demonstrate (i) they are being subject to online (first or third-degree) price discrimination and (ii) that said discrimination is occurring solely on the basis of their location.[67] This may become easier once the Omnibus Directive transparency requirement on OPP is transposed into Member-States' laws, especially if this leads to traders providing meaningful information to consumers about the variables considered by the pricing algorithm in cases where location is the sole one (which is unlikely to be the case).

More recently, the Geo-Blocking Regulation was approved to prevent "unjustified geo-blocking and other forms of discrimination based, directly or indirectly, on the customers' nationality, place of residence or place of establishment, including by further clarifying certain situations where different treatment cannot be justified under Article 20(2) of [the Services Directive]."[68] Unlike the Services Directive, it clearly states that it does not apply to purely internal situations, where all the relevant elements of the transaction are confined within one single Member State.[69] While Gerlick and Loizu argue that the Geo-Blocking Regulation "eliminates one conduit through which such practices are facilitated, notably, discrimination on grounds of the consumer's place of residence"[70] (restricted to the access of goods or services mentioned in Article 4(1) of the Regulation), Sears holds that the Regulation "does not mandate the complete harmonization of prices. Different prices, offers, and conditions may be given to customers in certain scenarios, so long as it is nondiscriminatory. For example, a business could sell a product for a different price in its physical stores as compared to its website."[71] In a recent EC-conducted screening of nearly 500 e-shops selling clothing and footwear, furniture and household items, and electric appliances, "One fifth of the flagged websites did not respect the Geo-blocking Regulation which allows consumers to shop from websites not delivering in their country of residence, provided they can get it delivered to an address in the country served by the trader i.e. the "shop like a local principle"."[72]

There are also other sectoral EU legal instruments (notably, in the air[73], maritime[74] and coach[75] transport sectors) which may grant specific protection to consumers against nationality or location-based OPP when accessing certain types of services.

All in all, and going back to the text of Article 21 CFREU, it is safe to say that the EU legislator has (to date), in what concerns its anti-discrimination acquis, fallen short of ensuring comprehensive protection to EU consumers against OPP based on assumedly commonly-used factors/unique characteristics, such as language, religion or belief, political or any other opinions, property (i.e., wealth or lack thereof), disability (or health condition), age or sexual orientation. One may also point out that the burden of proof incumbent upon customers/plaintiffs for demonstrating they have been subject to online price discrimination

[67] Sears, 'The Limits of' (n 5), 32.
[68] Article 1(1) Geo-Blocking Regulation.
[69] Article 1(2) Geo-Blocking Regulation.
[70] Gerlick and Liozu, 'Ethical and Legal' (n 5), 90.
[71] Sears, 'The Limits of' (n 5), 35.
[72] EC, *Press Release "Online shopping: Commission and Consumer Protection authorities urge traders to bring information policy in line with EU law"* [2020], available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_156, consulted on 3rd June 2020.
[73] Article 23(2) of Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community.
[74] Article 4(2) of Regulation (EU) No 1177/2010 of the European Parliament and of the Council of 24 November 2010 concerning the rights of passengers when travelling by sea and inland waterway and amending Regulation (EC) No 2006/2004.
[75] Article 4(2) of Regulation (EU) No 181/2011 of the European Parliament and of the Council of 16 February 2011 concerning the rights of passengers in bus and coach transport.

under the currently existing laws seems to be an almost insurmountable obstacle for consumers wishing to enforce their rights in this space.

Regardless of the political factors which led to the aforesaid legislative inaction[76] and the legally prescribed burden of proof rules, it is expected that the EU will continue to push for the abolition of all types of discrimination in the supply of goods and services with a consumer-oriented view and in line with the Treaties[77]. In the meantime, it is of paramount importance to analyze what alternative tools EU law offers to consumers against OPP, starting with privacy and data protection laws.

4. EU Privacy and Data Protection law: a big hurdle for OPP.

OPP involves the collection, analysis and mining of information about consumers who visit online shops. This may include, depending on the characteristics of each trader's pricing strategy (and the model of the pricing algorithm), personal data[78] such as the consumer's name, other unique identifiers (such as cookie IDs or their device's IP or MAC Address[79]), purchase history via loyalty cards or in the trader's website, email address, phone number, location (eg. GPS data and Bluetooth sensor data), type of device and browser used to access the online shop, publicly available data (eg. land registry records), behavioral and interests data (eg. browser history, apps used, social media posts) and socio-demographic data (eg. age, gender, level of education, number and identification of household members).

The advent of tracking and data analytics technologies, bolstered by advances in computing power and, thus, decreases in the cost of collecting, storing and analyzing vast amounts of data, made it interesting for traders to try to maximize their profits by deploying pricing algorithms These algorithms are arguably capable of estimating each online consumer's WTP based on online profile(s) drawn from connections between multiple data points[80].

---

[76] Back in 2008, the European Commission proposed the so-called Horizontal Directive, which intended to ensure equal treatment between persons in the EU, irrespective of religion or belief, disability, age or sexual orientation, including with regards to the access to goods and services. Since then, twelve years have passed and the legislative process did not lead to the adoption of the Directive, arguably because it has been blocked by the Council. See Proposal for a Council Directive on implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation {SEC(2008) 2180} {SEC(2008) 2181}, of 2nd July 2008. See also Joint NGO Statement on the 10th Anniversary of the Horizontal Directive, *Ten years on and nothing to show for it* [2018], available at https://www.age-platform.eu/sites/default/files/HorizontalDirective_jointStatement_10th%20Anniversary-Jul2018.pdf, consulted on 5th June 2020.

[77] For a comprehensive view of the currently applicable anti-discrimination framework in Europe, see European Union Agency for Fundamental Rights (FRA), *Handbook on European non-discrimination law* [2018].

[78] Article 4(1) GDPR.

[79] Recital (30) of the GDPR states that "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

[80] See Authority for Consumers and Markets Authority, *Guidelines on the Protection of the online consumer - Boundaries of online persuasion* [2020], available at https://www.acm.nl/sites/default/files/documents/2020-02/acm-guidelines-on-the-protection-of-the-online-consumer.pdf, consulted on 3rd June 2020, 19: "Technological developments are enabling businesses to predict consumer behavior with increasing accuracy using personal and other data. For example, businesses are increasingly well informed about consumers' personal preferences and choices, in some cases better than the consumers themselves." See also Gerlick and Liozu, 'Ethical and Legal' (n 5), 86: "Businesses race to convert mountains of data into generative insights to improve personalization-centered retail practices. They deploy internally developed and acquired technology factors that enable the marketing function to bridge from customer segmentation to individual personalization."

Frequently, the data collection, analysis and mining, as well as consumer profiling[81] and price targeting via a pricing algorithm will not be conducted by the traders themselves, but by service providers on their behalf, like data brokers and data analytics companies (as outlined in Chapter I). However, this does not relieve traders from complying with their obligations as data controllers[82] vis-à-vis the consumer personal data processing for OPP, given that, in any case, they define the purpose of the processing of said data[83]. The fact that, in certain cases where the consumer tracking technologies and the pricing algorithm models are defined by external service providers, traders may not determine or have visibility on some essential elements[84] of the means of the data processing for OPP may be troublesome in that regard. According to the EDPB, where a service provider takes an active role in determining said essential means and the purpose of the data processing, it acquires a certain degree of (sole or joint) controllership[85], even if it enters into an agreement with a trader which formally qualifies it as a mere processor[86]. In those cases (notably, where service providers do not reveal to their customers – i.e. traders – all the sources and types of data their "proprietary" pricing algorithm shall use to reach a pricing decision), it is still not clear, under recent CJEU case law, whether traders shall be acting as independent or joint

[81] For the purposes of the GDPR, 'profiling' is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." See Article 4(4) of the GDPR. The analysis and prediction of said aspects tend to have a decisive impact on pricing decisions taken by pricing algorithms. See I Mendoza and L A Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (2017) University of Oslo Faculty of Law Research Paper No. 2017-20, 1: "[Profiling] methods are instituted for a variety of ends, such as enhancing the impact of advertising, screening applicants for jobs or bank loans, and creating differentiated pricing for services. Examples include online behavioural advertising, e-recruiting, and weblining." Also, according to Mendoza and Bygrave (2), 'weblining' includes, but is not limited to, OPP.

[82] Article 4(7) GDPR defines 'controller' as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[83] Those obligations include, among many others, ensuring that only the types of personal data which are strictly necessary are processed, that a legal basis (eg. consent) exists for carrying out the processing, that consumers (as data subjects) are informed about how their data is processed, that the processing of sensitive personal data or automated decision-making affecting data subjects is not forbidden in a given case, that data subjects are given the possibility of opting-out of profiling and that all third-parties involved in the data processing are bound by specific duties relating to data protection.

[84] The EDPB has stressed that these 'essential means' "are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller" and include, *inter alia*, the determination of the types of data which shall be processed, the categories of data subjects, for how long the data will be retained, as well as who shall have access to the data. See EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* [2020], 9.

[86] As stressed by the EDPB, "a merely formal criterion would not be sufficient", as "it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing". It is also possible to imagine, in the context of OPP, "a processor [that] infringes the GDPR by going beyond the controller's instructions [by] starting to determine its own purposes and means of processing" (eg. if the personalization services provider decides to collect additional types of data to build more detailed consumer profiles and to train its "proprietary" pricing algorithm), thereby acquiring a controller status regarding those specific processing operations. See WP29, *Guidelines 07/2020* (n 86), 17 and 25, and Article 28(10) GDPR.

controllers[8788] with those service providers, in relation to the traders' website visitors' personal data. In the latter case, both parties would need to agree on which of them should inform consumers about the processing of their personal data for OPP purposes[89]. In cases where said service providers only define purely technical means[90] of the processing of the consumers' data for OPP purposes – thus firmly keeping their processor status –, traders may instruct those providers to assist them clarifying any questions consumers may have about the processing of their data by the pricing algorithm[91].

As controllers, for collecting and further processing (either directly or through third-party service providers) consumer data for OPP purposes, traders will need to make sure that a valid legal basis exists to that effect. While it is very unlikely that said processing may be considered necessary for entering into a contract with the consumer[92], and given that the WP29 has ruled out the possibility of relying on the legitimate interests' legal basis[93] for extensive profiling[94], "tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research"[95], it seems that traders have no choice but to rely on consumers' consent for OPP[96].

While the above is still open to some discussion (as controllers may admittedly still conduct some forms of non-intrusive profiling under the legitimate interests' legal basis), it is crystal clear that traders relying on tracking technologies which capture information from consumers' devices for OPP purposes (such as cookies, device fingerprinting or tracking pixels) must collect prior express[97] consent from the user, under Article 5(3) of the ePrivacy

---

87 It seems more likely that such service providers would be qualified as joint controllers with the trader deploying OPP in its website, since, in principle, they shall be determining certain essential elements of the means of one or more data processing operations involved in OPP and will use the data to train their pricing algorithm, therefore pursuing their own business interests. This is irrespective of the fact that personalization service providers shall tailor prices on the basis of data observed (eg. via tracking pixels or geo-targeting) or inferred (eg. from browser searches) about consumers.. See Judgement of 29th July 2019, *Fashion ID GmbH & Co. KG, C-40/17*, ECLI:EU:C:2019:629, paragraphs 77 to 84, and EDPB, *Guidelines 08/2020 on the targeting of social media users* [2020], 20 and 23.

88 It is safe to assume, however, that a given entity does not need to have access to the personal data to be considered as a controller jointly with the entity accessing the data, as long as both jointly determine the purpose and the means of the data processing. This shall often be the case of traders who employ personalization service providers for OPP purposes and never actually receive the raw data obtained and processed by said suppliers for that purpose. See Judgement of 10th July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 69.

89 Article 26(1) GDPR.

90 For instance, the way the data is stored in the providers' servers and protected against any risks, for the purposes of Article 32(1) GDPR, as well as the lines of code used to program the pricing algorithm strictly to fit the trader's pricing strategy.

91 Article 28(3)(e) GDPR.

92 See EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* [2019], 9: "When assessing whether Article 6(1)(b) [GDPR] is an appropriate legal basis for processing in the context of an online contractual service, regard should be given to the particular aim, purpose, or objective of the service. For applicability of Article 6(1)(b), it is required that the processing is *objectively necessary* for a purpose that is integral to the delivery of that contractual service to the data subject."

93 Article 6(1)(f) GDPR.

94 See WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217)*, of 9th April 2014, 18 and 26.

95 WP29, *Opinion 03/2013 on purpose limitation (WP203)*, of 2nd April 2013, 46.

96 With a similar view, see F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), 361; Sears, 'The Limits of' (n 5), 21; Gerlick and Liozu, 'Ethical and Legal' (n 5), 90; OECD (Directorate for Financial and Enterprise Affairs Competition Committee), *Personalised Pricing in the Digital Era – Note by the BEUC* [2018], 9; and Ministerie van Justitie en Veiligheid, *Moties op het terrein* (n 19), 4.

97 The CJEU has confirmed that the meaning of user "consent" in the ePrivacy Directive equates to the Article 4(11) GDPR concept of consent and, in line with Recital (32) GDPR, it ruled that pre-ticked checkboxes which are not un-ticked by a website user before continuing to browse the site do not constitute valid consent for the

Directive. A similar conclusion should be drawn where the trader processes the categories of personal data set-out in Article 9(1) GDPR – such as information revealing the consumer's racial or ethnic origin, religion, health condition or sexual orientation – for OPP purposes, even if those elements are merely inferred[98] from other data which are voluntarily provided by the consumer or observed by the trader[99] and regardless of whether said inferences are correct or not[100].

It is also highly discussed in academic literature whether OPP falls under the Article 22(1) GDPR definition of automated decision-making and, thus, whether OPP is forbidden, save for consumer explicit consent[101]. On the first issue, as rightly pointed out by Sears, "four conditions must be met for [Article 22] to apply. There must be (1) a decision (2) based solely (3) on automated processing of personal data that (4) results in legal or similarly significant effects on the individual."[102] If the fulfilment of the three first criteria by OPP is not contentious, authors have discussed whether OPP may have a legal or similarly significant effects on the data subject (in this case, the consumer being targeted with a personalized price). For Steppe, OPP does not have a legal effect on the consumer and shall only have a significantly similar effect in cases where the consumer is asked to pay a substantially higher amount[103]. More generously, Malgieri and Comandé take the view that the majority of pricing

placement of cookies or for using similar technologies. A similar argument should be drawn against the consideration of the mere display of an OPP tag, next to a personalized price, as any form of valid consent under the GDPR – it is not because a consumer has been shown an OPP tag that he or she accepts the processing of his or her personal by an intrusive pricing algorithm. See Judgement of 1st October 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH, C-673/17, ECLI:EU:C:2019:801, paragraphs 55, 57 and 63. In the same line, see AG Spuznar Opinion of 4th March 2020, *Orange România SA*, C-61/19, ECLI:EU:C:2020:158, paragraph 60. Subsequent processing of the personal data which may be obtained via a cookie, however, may, in theory, be based on alternative legal bases under Article 6(1) of the GDPR. See, in this regard, EDPB, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities* [2019], paragraph 41.

98 See Wachter & Mittelstadt, 'A Right to Reasonable Inferences' (n 17), 72: "when inferred or derived data directly disclose protected attributes—for example when a processor infers a person's ethnicity from their education history—they must be treated as sensitive data. (…) Second, when personal data can be shown to allow for sensitive attributes to be inferred (i.e., 'indirectly revealed'), the source data from which sensitive inferences can be drawn can also be treated as sensitive data (e.g. last name or location of birth to infer race)." See also WP29, *Advice paper on special categories of data ("sensitive data")*, Ref. Ares(2011)444105, of 20th April 2011, 6: "not only data which by its nature contains sensitive information is covered by [what today corresponds to Article 9(1) GDPR], but also data from which sensitive information with regard to an individual can be concluded."

99 On the distinction between inferred, observed and voluntarily provided data, see WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (*WP251rev.01)*, as last Revised and Adopted on 6th February 2018, 8; and Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 49.

100 In its Nowak ruling, the CJEU took a broad view on the definition of personal data, therein including data in the form of opinions and assessments, provided that they relate to the data subject. See Judgement of 20th December 2017, *Peter Nowak v. Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paragraph 34..

101 As Article 22(2)(a) and (b) GDPR are unlikely to be applicable in OPP involving automated decision-making.

102 See Sears, 'The Limits of' (n 5), 23.

103 R Steppe, 'Online price discrimination and personal data: A General Data Protection Regulation perspective' (2017) Computer Law & Security Review 33, 783. In agreement with Steppe, Bygrave claims that OPP shall only have such similarly significant effects with it represents "non-trivial economic consequences [for data subjects] (e.g. the data subject must pay a substantially higher price for services than other persons, effectively preventing her/him from accessing these services) – a fortiori if this occurs repeatedly". See L A Bygrave, *The EU General Data Protection Regulation (GDPR) – A Commentary* (1st edn, Oxford University Press 2020), 534. Both opinions seem to be in line with the position taken by the WP29 (and later embraced by the EDPB), as the latter holds that "For data processing to significantly affect someone the effects of the processing must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential

algorithms represent automated decision-making having a similarly significant effect on data subjects[104]. The Belgian DPA inclusively held, back in 2011 (pre-GDPR), that OPP even produces legal effects for consumers when they are required to pay a premium (regardless of its amount).[105] On the second contentious matter, it now seems clear that Article 22(1) GDPR contains a general prohibition on decision-making based solely on automated processing, and not a subjective right for data subjects to object to said decision-making[106], in spite of the fact that the wording of Article 22(1) could suggest that the latter was the case.

So, if data subject consent[107] is required for OPP, how should traders be planning to obtain it? Will we witness a proliferation of "OPP banners" in traders' websites, which would pop-up once a visitor accesses the site, asking him or her to consent to OPP (just like cookie banners do[108] in relation to analytics and advertising cookies)? This would add a degree of complexity to the Omnibus Directive-mandated "OPP tags" (which were discussed in Chapter II), as they would be serving an additional purpose to merely informing consumers about OPP.

Traders could also consider adding a new purpose[109] (i.e., data processing for OPP) to their currently used cookie banners, although this would only cover the use of tracking technologies for OPP and not the collection of their data through other means (eg. scrapping of publicly available data by data brokers), the combination of all those data for consumer profiling and, ultimately, price tailoring. In both those cases, traders should avoid implementing OPP or cookie-walls (i.e., denying access to the site unless the user accepts OPP or non-essential cookies[110]), "nudging" techniques (eg. placing a big, bright colored "Accept" button and a small, grey "Reject" button in the banner) and assuming that a user

---

to: significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals." See WP29, *Guidelines on Automated individual decision-making* (n 102), 21.

[104] G Malgieri & G Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) IDPL 7, 243.

[105] Commission for the Protection of Privacy Belgium, *Opinion no. 35/2012 of the CPP's accord on the draft regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, of 21st November 2012, unofficial translation www.privacycommission.be/sites/privacycommission/files/documents/Opinion_35_2012.pdf, consulted on 3rd June 2020, paragraph 80.

[106] See WP29, *Guidelines on Automated individual decision-making* (n 102), 19 and 20.

[107] Consent should be "freely given, specific, informed (…) unambiguous" and given "by a statement or by a clear affirmative action". See Article 4(11) GDPR.

[108] Or should do. While some DPAs have recently taken the view that some first-party analytics cookies may be exempt from the ePrivacy Directive's consent requirement (such an the French DPA), both the Irish and the UK DPAs have stressed that analytics cookies are not strictly necessary for providing an information society service at the request of the user and, as such, may only be placed upon prior user consent. See Commission Nationale de l'Informatique et des Libertés (CNIL), *Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019*, of 1st October 2020, available at https://www.cnil.fr/sites/default/files/atoms/files/ligne-directrice-cookies-et-autres-traceurs.pdf, consulted on 3rd October 2020; Data Protection Commission, *Guidance Note: Cookies and other Tracking Technologies* [2020], 7-8 ; and Information Commissioner's Office, *How do we comply with the cookie rules?*, available at https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply10, consulted on 4th June 2020.

[109] Matte, Santos and Bielova have denounced that websites relying on IAB Europe's Transparency and Consent Framework do not offer the user the possibility of consenting to the placement of cookies for purposes which are specific enough to meet the GDPR's purpose specification principle. See C Matte, C Santos, N Bielova, 'Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?' (2020) APF 2020 - Annual Privacy Forum, Oct 2020, Lisbon, Portugal, 1-24.

[110] See EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679* [2020], paragraphs 39 to 41.

who merely closed the banner without accepting or rejecting OPP or cookies has consented to their use[111]. In spite of all these requirements, it is possible that some consumers will still consent to the processing of their data for OPP purposes (in what is known as the 'privacy paradox'[112]), in particular if the consent request is worded in an engaging way[113], leading them to believe that OPP would never work to their disadvantage[114]. Another possible option for traders would be to have consumers consent to the processing of their personal data for OPP through an OPP browser setting, if this shows technically possible[115]. In any case, for consent to be informed, the EDPB has stressed that data subjects need to be provided with, at least, a minimum set of information elements, including the controller's identity, the types of data which will be collected and used and whether the data shall be used for automated decision-making under Article 22 GDPR[116]. However, providing this information through browser settings does not seem feasible in the current state-of-the-art[117]. Additionally, if traders decide to engage in OPP which falls under Article 22(1) GDPR or if it involves the processing or inferring of sensitive personal data[118], they will need to obtain an "explicit"

---

111 ibid paragraph 86. In a study published in April 2020, Nouwens and others show that only 11,8% of 10.000 analyzed websites in UK complied with the GDPR standards for valid consent for the placement of cookies. See Nouwens M and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (2020) CHI '20.

112 See F Zuiderveen Borgesius and others, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' (2017), EDPL 3, 6.

113 The UK DPA has stressed that "it may still be possible to incentivize consent to some extent. There will usually be some benefit to consenting to processing. For example, if joining the retailer's loyalty scheme comes with access to money-off vouchers, there is clearly some incentive to consent to marketing. The fact that this benefit is unavailable to those who don't sign up does not amount to a detriment for refusal. However, you must be careful not to cross the line and unfairly penalize those who refuse consent." See Information Commissioner's Office, *What is Valid Consent?*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what2, consulted on 21st May 2020.

114 As noted by Vieira Ramos, consumers tend to be overly optimistic, as they normally consider that negative events, such as paying a higher price than other consumers for the same product just because of what they have searched online earlier that week, are more likely to happen to others than to themselves. See M Vieira Ramos, 'Psicologia e Direito do Consumo' (n 45), 361.

115 While the CJEU has clarified that data subjects "cannot choose who is allowed to process their personal data once consent is given if the processing is covered by the original purpose of collection" (notably, if this purpose is OPP), the EDPB, in line with Recital (42) GDPR, has recently stressed that "[browser settings intended to collect consent for data processing] should be developed in line with the conditions for valid consent in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers." The CJEU's position seems to be more aligned with Article 6(1)(a) GDPR, however, since consent needs to be granted for specific purposes, not for specific controllers, even if controllers need to be able to demonstrate data subjects have consented to the processing of their data, under article 7(1) GDPR. See Laura Drechsler & Benito Sánchez, 'The Price is (Not) Right' (n 5), 4; Judgement of 14th October 2010, *Deutsche Telekom AG v Bundesrepublik Deutschland*, C-543/09, ECLI:EU:C:2010:603, paragraph 61; and EDPB, *Guidelines 05/2020* (n 113), paragraph 89.

116 See EDPB, *Guidelines 05/2020* (n 113), paragraph 64.

117 See Information Commissioner's Office, *op. cit.* note 105. Even if Recital (66) of the Cookie Directive suggests browser settings as a means of obtaining user consent for the placement of cookies, said option has been scrapped from the latest revised draft of the ePrivacy Regulation Proposal. See Council, DRAFT doc. st9931/20 on ePrivacy, available at <http://downloads2.dodsmonitoring.com/downloads/EU_Monitoring/2020-09-24_Projet_e-privacy_Allemagne.pdf>, consulted on 29 September 2020.

118 The wide catalogue of elements of information protected as special categories of data under Article 9(1) GDPR, whose processing is forbidden unless one of the exceptions in indent (2) applies, deems to prevent data subject discrimination based on their most sensitive personal attributes. This catalogue encompasses characteristics which are not specifically protected under EU secondary anti-discrimination law (see Chapter III, above), such as political opinions, religion health condition and sexual orientation.

consent, which amounts to a higher threshold of accountability[119].

For consent to be informed, in cases involving OPP falling under Article 22(1) – see above –, consumers need to be informed beforehand about the logic behind the pricing algorithm, as well as the significance and the envisaged consequences of OPP.[120] While this does not force traders to explain each individual pricing decision taken by the algorithm to consumers[121], they will need to explore "clear and comprehensive ways to deliver the information to the data subject, for example: the categories of data that have been or will be used in the profiling or [OPP] process; why these categories are considered pertinent[122]; how any profile used in the [OPP] process is built, including any statistics used in the analysis; why this profile is relevant to the [OPP] process; and how it is used for [the pricing decision].[123] Some traders may, however, feel tempted to convey the least possible amount of information to data subjects about these practices, with the justification that their pricing algorithm is protected under their fundamental freedom to conduct a business.[124]

On the "envisaged consequences" element, traders may wish to inform data subjects that the OPP process will lead to the price being reduced or increased up to a maximum of x% of the reference price or when compared to prices paid by other consumers, thus allowing for a conscious decision on whether or not to accept OPP.[125] Once more, traders will struggle with complying with this information duty if they are not fully aware of how the pricing algorithm works. Where the algorithm is developed by a third-party contractor without very precise instructions from the trader, the latter will likely need to ask the former for assistance with complying with GDPR information requirements. Contractors could, however, refuse to provide said assistance for trade secrecy reasons.[126]

As illustrated in this chapter, EU privacy and data protection law does not outright prohibit OPP, but places traders wishing to deploy it at a compliance crossroads. Firstly, the

---

[119] The difference between "express" and "explicit" consent is that the latter "requires a high degree of precision and definiteness in the declaration of consent, as well as a precise description of the purposes of the processing". See Bygrave, *The EU General* (n 99), 377. The EDPB adds that "The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. (…) For example, in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature." See EDPB, *Guidelines 05/2020* (n 113), paragraphs 93 and 94.

[120] See Articles 13(2)(f) and 14(2)(g) GDPR.

[121] Wachter, Mittlestadt and Floridi argue that the wording in the GDPR confers the data subject a right to *ex ante* explanations of [AI] *system functionality* (eg. the system's requirements specification, decision trees, pre-defined models, criteria, and classification structures), not the rationale and circumstances of *specific decisions* taken by the system. In the authors' view, Recital (71) GDPR confers a "non-binding right to an explanation of specific decisions after decision-making occurs". See S Wachter, B Mittelstadt & L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) International Data Privacy Law Vol. 7 No. 2, 82.

[122] On this, Drechsler & Benito Sánchez have claimed that this "could mean (…) that an individual subject to [OPP] receives information on what datasets are considered positively and what datasets are considered negatively for [the price which is presented to him/her]". See Laura Drechsler & Benito Sánchez, 'The Price is (Not) Right' (n 5), 12.

[123] See WP29, *Guidelines on Automated individual decision-making* (n 102), 31.

[124] On how the CJEU has been striking a balance between the controller's freedom to conduct a business and the data subject's fundamental right to data protection, see Judgement of 29th January 2008, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54, paragraphs 62 to 70.

[125] See Information Commissioner's Office and The Alan Turing Institute, *What goes into an explanation?* [2020], available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence/part-1-the-basics-of-explaining-ai/what-goes-into-an-explanation/, consulted on 4th June 2020.

[126] See note 17.

distribution of roles and responsibilities between traders and their OPP suppliers with respect to the processing of consumers' data is not clear. Secondly, the processing of consumer data for OPP purposes generally requires prior consent from the data subjects (consumers), which they will possibly not grant if they are properly informed about how OPP works. Thirdly, as data controllers, traders must comply with cumbersome information duties towards consumers who are subject to OPP, which require them to understand how their pricing algorithms work. With DPAs across the EU increasingly focusing on cookie rules enforcement[127] and algorithmic discrimination[128], traders are bound to be taking a careful look into if and how they shall pursue OPP practices.

To top it off, traders deploying pricing algorithms – even those complying with data protection rules and the new Omnibus Directive transparency requirement – will need to ensure their OPP does not constitute a forbidden unfair commercial practice. This is analyzed in the ensuing chapter.

5. OPP as an Unfair Commercial Practice?

The UCPD lays down the rules on commercial practices which, given their unfair, misleading or aggressive nature, traders are not allowed to pursue. Some examples of these restricted practices are "falsely stating that a product will only be available for a very limited time", "presenting rights given to consumers in law as a distinctive feature of the trader's offer" or telling the consumer that "if he does not buy the product or service, the trader's job or livelihood will be in jeopardy"[129]. Although the Omnibus Directive introduced some amendments to the UCPD, these are not directly relevant for addressing OPP's compliance with the UCPD[130].

Although it is true that OPP per se does not seem to constitute an unfair commercial practice, forbidden under the UCPD[131], the EC has highlighted that "personalized pricing/marketing could be combined with unfair commercial practices in breach of the UCPD"[132].

It is possible to envisage how OPP could constitute a misleading commercial practice, under Article 6(1)(d) UCPD[133], notably where the trader, when complying with the novel Omnibus Directive transparency requirement regarding OPP, falsely informs the consumer that the pricing algorithm will always show him lower prices than what the trader would offer in case the pricing algorithm were not used[134]. On whether this particular practice would

---

[127] See Bird&Bird, *The Spanish Data Protection Authority fines Vueling with 30,000 euros for failing to comply with cookie rules*, October 2019, available at https://www.twobirds.com/en/news/articles/2019/spain/la-aepd-ha-impuesto-a-vueling-una-multa-de-30000-euros, consulted on 4th June 2020.

[128] See CNIL, *Algorithmes et discriminations : le Défenseur des droits, avec la CNIL, appelle à une mobilisation collective, 2nd June 2020*, available at https://www.cnil.fr/fr/algorithmes-et-discriminations-le-defenseur-des-droits-avec-la-cnil-appelle-une-mobilisation, consulted on 4th June 2020.

[129] See Annex I of the UCPD.

[130] Nonetheless, the Omnibus Directive does create possibilities for consumers to access "proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract." The right of having the price for a good or service reduced after becoming aware that the price algorithm worked to their disadvantage (contrarily to what traders may advertise), could serve as a useful tool for consumers targeted by OPP. See Article 4(5) Omnibus Directive.

[131] See Sears, 'The Limits of' (n 5), 16.

[132] See EC, *Staff Working Document* (n 20), 134.

[133] Which forbids the trader to inform the consumer in a deceitful (or likely deceitful) manner about the product's or service's price or the manner in which the price is calculated.

[134] See Authority for Consumers and Markets Authority, *Guidelines on the Protection of the online consumer* (n 82), 25.

likely deceive the average consumer[135] and could cause him to take a transactional decision[136] that he/she would not have taken otherwise, there are good arguments to support a positive answer: given that the average consumer is price-oriented and not really aware of how OPP works[137], any indication given by the trader that he/she will be always granted a discount in case he/she accepts OPP is likely to lead the consumer to accept OPP and even to purchase products and services from the trader that he/she would otherwise not.

OPP could also be associated with a misleading omission under Article 7(1) or (2) UCPD. If a trader does not inform the consumer that the price he/she is being offered in the online shop has been calculated by a pricing algorithm (in breach of the new transparency duty stemming from the Omnibus Directive), or does so in an "unclear, unintelligible, ambiguous or untimely manner", this should be regarded as a misleading omission[138]. In fact, since the enactment of the Omnibus Directive – making the provision of information about OPP mandatory for traders – this should be considered "material information" for the purposes of those provisions of the UCPD, which needs to be given to consumers to allow them to take a conscious decision about whether or not to engage with traders deploying pricing algorithms[139]. This is so even today, before the Omnibus Directive has been transposed by the EU Member-State where the consumer has his/her habitual residence[140] or before 28th November 2021 (the deadline for transposing the Omnibus Directive[141]), as – in line with CJEU case law – national law transposing the UCPD should be read under the light and in accordance with Directives (such as the Omnibus Directive) which lay down a general principle of EU law (like consumer protection), even before their transposition deadline has elapsed[142].

---

135 I.e., one "who is reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors". See Recital (18) UCPD.

136 As clarified by the EC, a 'transactional decision', for the purposes of Article 6(1) UCPD, does not necessarily mean the decision of purchasing or not purchasing a product or service, but may also be a pre-purchase or post-purchase decision, such as a decision to click through a webpage as a result of a commercial offer. See EC, *Staff Working Document* (n 20), 33-35.

137 See Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 103: "The self-reported awareness about *online personalised pricing* was on average quite lower than the self-reported awareness about online targeted adverts and personalised ranking of offers. Across the EU28, slightly more than four in ten (44%) of respondents reported to understand or have some understanding of how personalised pricing used by online firms works. In contrast, nearly 3 out of 10 (29% of) respondents mentioned that they hadn't heard of it up until now (versus only 8% and 11% for targeted advertising and personalised ranking of offers, respectively).

138 In order to avoid this, traders may wish to follow the WP29 information-provision checklist about automated decision-making, when delivering information to consumers about OPP. See Chapter IV and WP29, *Guidelines on Automated individual decision-making* (n 102), 31.

139 Even where the pricing algorithm would normally benefit the consumer at stake, by offering him/her a lower price than to most other consumers. See Miller, 'What Do We Worry' (n 1), 85; and Priester, Robbert and Roth, 'A Special Price' (n 3), 104 and 105.

140 Under the Rome I Regulation, this should be, as a rule, the law applicable to contracts concluded between traders and consumers. See Article 6(1) of Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations.

141 Article 7(1) Omnibus Directive.

142 In Mangold, the CJEU awarded horizontal indirect effect to a Directive which deemed to ensure equal treatment (in particular, non-discrimination based on age) in the field of employment and occupation, even before the deadline for transposal of the Directive had elapsed. On that occasion, the Court held that non-discrimination on grounds of age "must be regarded as a general principle of [EU] law" and, thus, its observance "cannot as such be conditional upon the expiry of the period allowed the Member States for the transposition of a directive intended to lay down a general framework for combating discrimination on the grounds of age". On a generous reading of said judgement, one may argue that Article 4(4)(ii) of the Omnibus Directive intends to lay down a provision for ensuring consumer protection vis-à-vis OPP, and that consumer protection is also a general principle of EU Law, under Article 6(1) and (3) of the Treaty on European Union – as it is enshrined in Article 38 CFREU –, and, thus, the same rationale could apply to interpreting current Member-State law

Moreover, the Dutch Authority for Consumers and Markets (ACM) has recently raised the possibility of certain OPP strategies being considered as aggressive commercial practices, for the purposes of Article 8 UCPD. As an example, the ACM mentions a trader who misuses its "knowledge of a consumer's vulnerable circumstances [eg. acquired through insights provided by data brokers or by cookies tracking the consumer's browsing through fast, easy and high-interest credit providers' websites], possibly by offering products on instalment credit to financially vulnerable and/or indebted consumers"[143].

Even if certain OPP practices do not qualify as misleading actions or omissions, nor as aggressive commercial practices, they may still be considered as unfair commercial practices under the Article 5(2) UCPD 'safety net'. However, in this case, OPP practices would need to be assessed against the requirements of professional diligence, i.e., "the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity"[144]. Additionally, for it to be forbidden, OPP would need to, in a given case, be liable to materially distort the economic behavior of the "average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers"[145] Although this latter criterion seems fitting for assessing the fairness of third-degree online price discrimination practices, the same cannot be said of OPP, which is specifically targeted to individual consumers, and not to groups of consumers. Therefore, the "average consumer" criterion seems inadequate to evaluate the fairness of a given OPP practice, given the nature of OPP. In this regard, special mention to Article 5(3) UCPD should also be made. The provision reads that "Commercial practices which are likely to materially distort the economic behavior only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity[146] in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group". In cases of third-degree online price discrimination where the trader uses a pricing algorithm to target children with predatory prices, for instance, it would be more likely that the trader could foresee that this pricing strategy would impact those vulnerable consumers in a manner incompatible with Article 5 UCPD. But, once again, for cases of OPP, it would be more appropriate to have the trader consider the particular vulnerability (eg. an alcohol addiction or economic exposure inferred from repeated detection of the consumer's GPS location at a given liquor store or low-income neighborhood) of the specific consumers targeted with personalized prices, taking into account the information at its disposal about said consumers. All in all, the "average consumer" criterion appears outdated when assessing the fairness of OPP

transposing the UCPD in conformity with the new OPP-related transparency requirement. Judgement of 22nd November 2005, *Werner Mangold v Rüdiger Helm*, C-144/04, ECLI:EU:C:2005:709, paragraphs 75 and 76. See also Judgement of 14th May 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities*, 4-73, ECLI:EU:C:1974:51, paragraph 13; and Judgement of 26th February 2013, *Åkerberg Fransson*, C-617/10 ECLI:EU:C:2013:105, paragraphs 20 and 21.

[143] See Authority for Consumers and Markets Authority, *Guidelines on the Protection of the online consumer* (n 82), 25.

[144] Article 2(h) UCPD. It would likely be against professional diligence for traders to not inform consumers about OPP, thereby significantly impairing their freedom of choice of not engaging with traders deploying pricing algorithms. See Judgement of 26th October 2016, *Canal Digital Danmark A/S*, C-611/14, ECLI:EU:C:2016:800, paragraph 55.

[145] Article 5(2)(b) UCPD.

[146] The vulnerability factors outlined in Article 5(3) may not be exhaustive, given the wording of Recital (19) UCPD, which uses the expression "such as". According to Vieira Ramos, "situations such as [the consumer's] socio-economic condition, lack of experience, knowledge or habilitations also constitute important sources of vulnerability". See M Vieira Ramos, 'Psicologia e Direito do Consumo' (n 45), 449.

under Article 5 UCPD, which hints at the need of replacing or complementing it with a more suiting one.

Before presenting the paper's conclusions, it should be stressed that the application of the UCPD rules to OPP practices remains mostly untested by national courts and the CJEU, and that further clarity as to how the Directive's concepts apply to this relatively new practice is needed.

Conclusions.

As this paper tried to show, no matter how much consumers seem to dislike OPP, this practice is not outright forbidden under EU law and does not seem to be going away anytime soon[147].

Online price discrimination grounded on consumers' specially protected characteristics (such as gender, race, nationality or place of residence), in turn, is prohibited under EU certain (limited) anti-discrimination instruments, unless traders can provide objective justification for price differentiation based on said features. The burden of proof about the existence of discrimination, however, lies with the consumer/plaintiff, which may ultimately render these tools ineffective when a complex pricing algorithm decides considering various personal attributes which are fed to it about consumers.

The new transparency requirement brought by the Omnibus Directive in relation to OPP will shed light on this practice for consumers, which ought to be informed, in a clear and prominent manner and directly before clicking 'buy', about whether the price they are seeing when buying online has been tailored to their online profile(s) by a pricing algorithm. This warning must be written in a plain and intelligible language, every time a personalized price is offered, thus allowing the consumer to understand how OPP shall work in each case it is used. Further guidance from consumer protection bodies is needed to understand what level of detail of information should be conveyed to consumers in OPP tags. The upcoming EU instrument on AI could also consider pricing algorithms as "high-risk" AI applications, thus mandating enhanced transparency requirements in this regard towards consumers and regulators.[148]

European privacy and data protection places heavy incumbrances on traders wishing to collect and further process consumer data for OPP purposes. In general, this requires traders to obtain prior free and express consent from consumers, and to inform them about how the pricing algorithm will use their data to target them with personalized prices. Trade secret justifications may impede traders from receiving assistance from contractually engaged data brokers or data analytics companies with complying with said obligations, as well as from giving consumers meaningful information about the consequences OPP entails for their legal or financial interests.

Lastly, traders supplying false, incomplete or untimely information to consumers about OPP could face consequences from a consumer law perspective – notably, by having to offer a price reduction to consumers whose price was personalized –, as those may amount to misleading actions or omissions under the UCPD. The "average consumer" criterion seems to be of little use for assessing whether a commercial practice such as OPP – which, by its nature, is addressed to a specific consumer, and not to larger or narrower groups of consumers – is unfair for the purposes of the UCPD.

---

[147] O Bar-Gill, 'Algorithmic Price Discrimination When Demand Is a Function of Both Preferences and (Mis)perceptions' (2018) The University of Chicago Law Review, available at https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3184533_code837010.pdf?abstractid=3184533&mirid=1, consulted on 4th June 2020, Section I.A.

[148] EC, *White Paper On Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final [2020].

Enforcement of and further guidance on the rules applicable to OPP by Equality Bodies[149], DPAs and Consumer Protection Authorities is expected and needed to understand if traders deploying pricing algorithms will be subject to legal scrutiny as tight as the one being exerted by scholars. But also to see whether regulators and courts will award it the same "tolerance" as people tend to concede when they realize they have paid a different price than other consumers due to their recent whereabouts or Facebook likes.

[149] "The European Network of Equality Bodies (Equinet) promotes equality in Europe by supporting and enabling the work of national equality bodies, bringing together 46 organisations from 34 European countries. The EU equal treatment legislation requires Member States to set up an equality body to provide independent assistance to victims of discrimination. Most Member States have implemented this requirement, either by designating an existing institution or by setting up a new body to carry out the tasks assigned by the new legislation. However, no specific guidelines exist for Member States on how these bodies should operate. So far, European antidiscrimination law only requires that equality bodies are set up in the fields of race, ethnic origin and gender. Many countries have bodies that deal with other grounds of discrimination as well." See FRA, *Handbook* (n 79), 25.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Smart toys and minors' protection in the context of the Internet of everything

MARIA CRISTINA GAETA
Research Fellow in Private Law at the University Suor Orsola Benincasa of Naples
Lawyer in Naples

Abstract

Smart toys are devices with the appearance of traditional children's toys (e.g. dolls or cuddly toys) but they are capable of interacting with the surrounding environment, connecting to the Internet and using technological systems. They are robots, characterized by a more or less developed level of automation, to the point that the most recent models of connected toys are equipped with artificial intelligence. Although smart toys are fun and sometimes even educational games, they are still tools that collect, process and communicate data, with possible risks, especially for minors. Indeed, first of all it is very concrete and serious the risk of unlawful processing of minors' personal data, but also the risk of hacker attacks, issues related to possible emotional bonds between the minor and the toy, as well as psychical manipulation.

This paper will deepen the concept of smart toys, starting from the characteristics and the technical aspects and then moving on to the analysis of their possibilities and risks, in order to identify the possible legal remedies to be foreseen for protecting minors.

Keywords: Smart toys - IoToys - data protection - minors - GDPR.

Summary: 1. Characteristics and peculiarities of smart toys. – 2. Risks of smart toys. – 2.1. Minors' personal data processing through an IoToy. – 2.2. Smart toys' cyberattacks. 2.3. Ethical issue related to smart toys: from the emotional bonds to the psychological manipulation. – 3. Current regulation for minors' protection as vulnerable subjects in relation to new technologies. – 3.1. The evolution of the category of personality rights in the digital era. – 3.2. The civil regulation applicable to smart products. – 4. Conclusions: The need for effective preventive and remedial measures.

1. Characteristics and peculiarities of smart toys.

In the 21st century, the impact of new technologies is enormous. Technologies have changed the way of life of the human being, from personal relationships to work activities. On one side, new technologies represent an evolution but, on the other side, this evolution has to be regulated in order to put technologies at the service of man and not the opposite. Indeed, human beings are constantly monitored through the growing number of identification and tracking technologies and, in some cases, their behaviour is already influenced by the (ab)use of smart devices.

In this scenario characterised by the quick evolution of technologies, Internet development has played a central role which has been enhanced by the extension of this network to the world of objects, giving birth to the phenomenon known as the Internet of Things (IoT).[1] This information architecture has been defined as a network which connects

[1] With regard to the introduction of the term Internet of Things K Ashton, 'That "Internet of Things" Thing. In the real world, things matter more than ideas' (2009) RFID J, 1; S Haller, S Karnouskos, C

tangible or intangible goods, that becomes recognisable and can also acquires intelligence through the ability to collect and communicate data about themselves and the surrounding environment.[2] For their peculiarities, these objects are well known as 'smart things'.[3] Indeed, they are capable of interacting with the surrounding environment, connecting to the Internet and using a different kind of technological systems which change in accordance with the types of intelligent object. Nowadays, included in this category are incredibly wide kinds of objects developed in different sectors. So, in the smart mobility sectors, there are things such as ADAS or even highly automated vehicles,[4] in the medical sector,[5] instead, the intelligent medical equipment develops more and more quickly from the field of prostheses to the machinery needed to implant them, while, in the domotics sector,[6] we have for example intelligent thermostats or refrigerators. Regarding private life sector, then, are very spread smartphones but also smartwatches and, finally, in the recreational sector, not very known but problematic, are included the so-called smart toys for kids and teenagers, which will be the topic of this articles. There are so many smart things in the world that the concept of "Internet of Things" has moved to that of 'Internet of everything'.[7]

Reaching now the heart of the article, it is necessary to give a more precise definition of smart toys. Smart toys are part of the macro-category of smart things, connected online in

Schiroh, 'The Internet of Things in an enterprise context' (2008) Future Internet, Lecture Notes in 5468 Computer Science, 1. About Internet of Things definition, instead, *see* S Ziegler (ed), *Internet of Things Security and Data Protection* (Springer, 2019); G Noto La Diega, I Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 219 Queen Mary School of Law Legal Studies Research Paper; SR Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93 Texas Law Review, 85 ff.; RH Weber, 'Internet of Things, New security and privacy challenges' (2010) Computer law & security rep, 23 ff..

[2] European Research Cluster on the Internet of Things (IERC), Internet of Things Strategic Research Roadmap (2nd edn. 2011) 10, http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf, accessed 27th November 2020.

[3] Smart things are tagged with a Radio Frequency Identification (RFID) tag with a single ID called Electronic Product Code (EPC). About RFID *see* EK Pallone, "'Internet of Things" e l'importanza del diritto alla privacy tra opportunità e rischi' (2016) 17 (55) Ciberspazio e diritto, 174 f..

[4] On self-driving cars legal regulation *see* A Bertolini, M Riccaboni, 'Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules' [2020] Eur J Law Econ, 1 ff.; E Al Mureden, "'Autonomous cars e responsabilità civile tra disciplina vigente e prospettive de iure condendo' (2019) 3 Contr. impr., 2019, 895 ff.; U Ruffolo, E Al Mureden "'Autonomous vehicles" e responsabilità nel nostro sistema ed in quello statunitense' (2019) 7 Giur. It., 1657 ff.; A Albanese, 'La responsabilità civile per i danni da circolazione dei veicoli ad elevata automazione' (2019) 4 Europa e diritto privato, 995 ff.; A Davola, R Pardolesi, 'In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?' (2017) 5 Danno e responsabilità, 616 ff.. Please, allow me to refer to MC Gaeta, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies* (ESI, 2019). B Von Bodungen, IA Caggiano, H Steege, MC Gaeta (eds), *European regulation for self-driving cars* (Springer) (forthcoming).

[5] On the implementation of Robotics and AI in the medical sector, with specific reference to wearable robotics, *see* M Cardona, V Kumar Solanki CE García Cena (eds), *Internet of Medical Things. Paradigm of Wearable Devices* (Routhledge, 2021, forthcoming).

[6] *See* L Vizzoni, 'Dispositivi domotici e dati personali: dalle difficoltà applicative del GDPR alla prospettiva del futuro regolamento e-privacy' (2020) 4 Nuove Leggi Civ. Comm., 1032 ff.; F Pizzetti, 'Domotica. L'intelligenza artificiale che ci spia a casa: quali rischi e soluzioni per la privacy', available at https://www.agendadigitale.eu/sicurezza/privacy/lintelligenza-artificiale-che-ci-spia-a-casa-quali-rischi-e-soluzioni-per-la-privacy/, accessed 2nd December 2020.

[7] *See* B Di Martino, K Ching Li (et al.), *Internet of Everything. Algorithms, Methodologies, Technologies and Perspectives* (Springer, 2018); D Evans, 'Internet of Everything: Harnessing an Exponentially More Powerful Internet' (2012) Cisco Blog, available at https://blogs.cisco.com/digital/internet-of-everything-harnessing-an-exponentially-more-powerful-internet-ioe-infographic, accessed 2nd December 2020.

the IoT, and this is why they are also called Internet of Toys (IoToys).[8] They are devices with the appearance of traditional children's toys (e.g. dolls or cuddly toys) but they are capable of interacting with the surrounding environment, connecting through the Internet and using technological systems that range from sound systems (e.g. microphones), to visual systems (e.g. cameras), passing through the multiple types of sensors of movement or localisation, with which they are equipped. Interactive toys are robots, characterized by a more or less developed level of automation, to the point that the most automated models of connected toys can be equipped with artificial intelligence (AI).

Smart toys are, therefore, designed to interact actively with children and are often able to automatically perform various activities, such as recording sounds, taking photos or shooting videos, and sharing this data online (websites or social networks). The most advanced toys, then, include remote video control, gesture-based interactions, voice recognition and face tracking. Furthermore, smart toys can have medical sensors that monitor children's body temperature, heart pressure, blood values, and breathing.

Considering the fast and constant evolution of robotics and AI, machine learning and big data analytics, in all their applications, it is clear that these connected toys will continue to increase and evolve quickly bringing with them advantages but also serious risks.

2. Risks of smart toys.

2.1. Minors' personal data processing through an IoToy.

Although smart toys are fun and sometimes even educational games or toys capable of monitoring children's vital functions, they are still tools that collect, process and communicate information and personal data,[9] with consequent possible risks, especially for minors. Indeed, in relation to toys connection, there is a concrete risk of unlawful processing of minors' personal data, but also the risk of hacker attacks. Furthermore, problems related to possible emotional bonds between the child and the toy, as well as damages arising from a malfunctioning of the smart toy, can be configured. In this subparagraph all these risks will be in-dept, but let proceed with order, starting with the data protection issue.

Today, personal data, including that of the children are processed in huge quantities, that continuously grow and are updated, and that can be structured (such as date from databases) but also semi-structured or completely unstructured such as email obtained from profiles, images on social networks and GPS data. This is such a large amount of data that they are known as big data, i.e. a data set so extensive in terms of volume, speed and variety that requires specific analytical technologies and methods for the extraction of value or knowledge. This phenomenon is developing more and more quickly in recent years following

[8] About the definition of 'Internet of Toys' *see* European Commission, Joint Research Centre, Technical Reports, Kaleidoscope on the Internet of Toys, 2017; G Mascheroni, D Holloway (eds), *The Internet of Toys. Practices, Affordances and the Political Economy of Children's Smart Play* (Springer, 2020); L Green, D Holloway, 'Discursive constructions of the internet of toys' (2017), in 'Refereed Proceedings of the Australian and New Zealand Communication Association Conference. Communication Worlds: Access, Voice, Diversity, Engagement', available at https://ro.ecu.edu.au/ecuworkspost2013/4496/, accessed 3rd December 2020, L De Carvalho, M Eler, 'Security Requirements for Smart Toys', in Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017), Vol. 2, 144 ff..; C Tschider 'Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age' (2018) 96 (87) Denv. U. L. Rev., 120 ff.

[9] About privacy and smart toys *see* T Milosevic, P Dias, C Mifsud, CW Trültzsch-Wijnen, 'Media Representation of Children's Privacy in the Context of the Use of "Smart" Toys and Commercial Data Collection' (2018), 9 Media Studies, 26 ff..

the contextual rapid evolution of new technologies.[10]

The reasons why minors' personal data are processed are different. Of course, data are processed to guarantee the functioning of their operating system. Indeed, the operative systems works thought data to provide services for which they were designed (e.g. measure blood pressure or calculate the right body weight for that single child to whom the toy is given) or to provide better tailored services by analysing personal data relating to the child's interests and preferences (i.e. profiling him or her). However, there are other reasons for minors' data processing through IoToys.

About the domain of the marketing activities, personal data are used to profile minors (art. 4, para 1, n. 4, GDPR), i.e. any form of automated processing with the aim to analyse or predict minors' personal preferences, interests, health, behaviour and location, in order to offer directly to them via targeted ads, or put on the market, good and services in line with their profile.[11] The kind of data analysis related to the behaviour, go through the name of data commercialization practices and, in particular, is behavioural advertising or behavioural targeting, because is based around the behaviour of the users, usually online. Moreover, the behavioural advertising is so sophisticated activity that affects human being's and, especially, children, manipulating their choices and, in this case, their interests in purchasing of products and services.

In addition to this, minor's personal data processing can be used for potentially discriminatory practices, such as excluding children with certain profiles from particular types of education or refusing to grant specific health care or insurance policies on the base of the data collected. These forms of discrimination are made possible by the knowledge of the most intimate aspects of the person (special categories of personal data), such as those suitable for revealing the state of health, sexual orientation or ethnic origin.

An example of particular relevance regarding the unlawful processing of the minor's personal data concerns the case of 'Hello Barbie'. 'Hello Barbie' is an interactive doll produced by Mattel Inc., which features a computer chip, microphone, speaker and is Wi-Fi

---

[10] A definition of big data is provided by A De Mauro, M Greco, M Grimaldi, 'A Formal definition of Big Data based on its essential features' (2016) 63(3) Library Review, 122 ff. Down a legal point of view with particular regard to data protection egal issues, *see* Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, T-PD(2017)01; Italian Competition Authority, Italian Authority for Communications Guarantees and Italian Data, Guidelines and policy recommendations for Big Data, July 2019. Literature on the topic: A Mantelero, 'Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework' (2017) Computer Law and Security Review, 584 ff.; A Mantelero, 'La privacy all'epoca dei Big Data', in V Cuffaro, R D'Orazio, V Ricciuto (eds) *I dati personali nel diritto europeo* (Giappichelli, 2019), 1181 ff.; G D'Acquisto, M Naldi, *Big Data e Privacy By Design* (Giappichelli, 2018); A Mantelero, La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence, in A Mantelero, D Poletti (eds), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (Pisa University Press, 2018), 289 ff.; A Mantelero, 'Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo' (2012) 1 Dir. Inf., 135 ff..

[11] On risks and remedies of the automated decision making, including profiling process through the analysis of the data collected online, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe, Guidelines on Artificial Intelligence and Data Protection, 25 January 2019, T-PD(2019)01. The guidelines follow and are based on a Report by A Mantelero on Artificial Intelligence and Data Protection: Challanges and Possible Remedies of the same Consultative committee, of 25 January 2019, T-PD(2018)09Rev. *See* also A Mantelero, 'Regulating AI within the Human Rights Framework: A Roadmapping Methodology' in P Czech , L Heschl, K Lukas, M Nowak and G Oberleitner (eds), *European Yearbook on Human Rights 2020*, (Intersentia, 2020) 484 ff.; A Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: from an Individual to a Collective Dimension of Data Protection' (2016) 32 Comp. Law & Secur. Rev., 238 ff..

enabled. By pressing her belt, the doll asks a question and records the child's response. The message is encrypted and sent via the Internet to be processed by the voice recognition software of ToyTalk, Inc. (now PullString, Inc.), a partner of Mattel Inc.. The software then sends a command to Barbie to play an answer chosen among those stored in the doll which results appropriate according to the topic the child wants to talk about. What is of concern is privacy: the secrets confided to the doll by a child are shared with Mattel and its medical partners and could be illegally treated, even for discriminatory purposes. In addition, hackers are able to steal data processed by Hello Barbie, such as names, addresses, email and sensitive data from millions of families around the world. Hackers are also able to extract the name of the Wi-Fi network, the internal MAC address, the account ID and MP3 files, that are enough to get access to the Hello Barbie account and a home network.[12]

The legal protection of minors' personal data is contained in different international, European and national regulations that deal with internet minors and privacy,[13] among these a role of primary importance is covered by the new European regulation on data protection (GDPR).[14] Indeed, minors are data subjects that, knowingly or unknowingly, disclose information about themselves. They fall into the category of particularly vulnerable subjects, precisely because of their tender age which implies reasoning skills not completely defined and less awareness of their data processing.[15] The protection of the privacy of minors is an extremely important and topical topic in particular when the same processing takes place through new technologies tools and this contribution deals with the case in which the processing of minors' personal data takes place through smart toys. In this context, it is, therefore, necessary to establish when and how minors or their parents are informed about the processing of minors' personal data and what the legal basis for the lawful data processing.

The information on the processing of minors' personal data, included that related to profiling processes, should be drawn up in compliance with the provisions of articles 13 and 14 GDPR. This information should be provided in a privacy policy provided by the seller of the smart toy or it should be included in the software of the toy and appear at its first installation. Among the contents to be necessarily included in the privacy policy there are also the rights of the data subject (art. 12 - 23, GDPR), have also the function of preventing the discriminatory processing mentioned above.

The GDPR requires owners to demonstrate that the correlations applied in the algorithm are impartial, i.e. non-discriminatory and that there is a legitimate justification for the automated decision. Individuals subject to the automated decision, in fact, have a plurality of rights, such as opposition to profiling (Article 21), the request for cancellation or the rectification of their profile (Article 17), the challenge to automated decisions (Article 22, paragraph 3).

With specific regard to the content of the privacy policy, it must be emphasized that it is

---

[12] *See* ID Manta, IS Olson, 'Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly' (2015) 67 Alabama Law Review, 135 ff.. From a comparative point of view, *see* M Fantinato, PCK Hung (et al.), 'A preliminary study of Hello Barbie in Brazil and Argentina' (2018) 40 Sustainable Cities and Society, 83 ff.. More recently, starting from 2017, a new Barbie model, Barbie hologram, was designed but no studies have yet been published on it.

[13] IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (2018) 1 Familia, 7 ff.; F. Scia, *Diritti dei minori e responsabilità dei genitori nell'era digitale* (ESI, 2020), 17 ff..

[14] Regulation 2016/679/EU of the European parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR) [2016] OJ L119/1.

[15] In this sence rec. 38 GDPR.

not enough to include the information requested by the GDPR, but a greater effort is needed in order to guarantee an adequate level of awareness of the data subject, especially of the minor. In order to implement minor awareness, it should be necessary to simplify the privacy policy, in the double direction of limiting the contents to those strictly necessary according to article 13 and 14 of the GDPR and explain them in the simpler and effective way in relation to the category of data subject involved, which does not only concern the language used but also how the information is represented graphically. Regarding the information, the privacy notice must contain information that is concise, transparent,[16] intelligible, easily accessible and to understand, as well as written in clear and plain language, according to the first paragraph of the article 12 and the recital 58 of the GDPR. Additionally, where appropriate, visualization principles can be used for the organization of the information contained therein. Indeed, the paragraph 7 of the article 12 of GDPR states that information can be provided in combination with standardised icons, in order to help the data subject to know and understand whether, by whom, for what purpose and how long his or her personal data are being processed.[17]

On the other hand, in relation to the legal basis of the processing, the same could be based on the data subject consent or, in some cases, to the performance of a contract of which the data subject is a party. GDPR provides, as one of the legal basis, the rule of the express consent of the processing of personal data (art. 6, para 1, let a), GDPR) with the exception constituted by the explicit consent, required only with regard to special categories of personal data (art 9, para 2, let a), GDPR), profiling activities included the above mentioned (art. 22, para 2, GDPR), to which is added the case of the transfers of personal data to a third country or an international organisation (art. 49, para 1, lett. a), GDPR).[18]

About minors' consent to the processing of personal data, the GDPR provides specific discipline, in particular, it is envisaged that they can provide consent to the processing of their personal data with regard to the processing through the information and

[16] Concerning the transparency processing *see* Article 29 WP, Guidelines on transparency under Regulation 2016/679, 11th April 2018, no. 260. During its first plenary meeting the EDPB endorsed the GDPR WP29 Guidelines on transparency.

[17] About the icons that could be included in a privacy policy, the first reading of the European Parliament on COM (2012)0011, was supplemented by an Annex containing an iconic privacy policy. This annex, indeed, provided, standardised icons that would have been helpful to understand the information contained in the privacy policy. However, the annex has been eliminated in the final version of the GDPR proposal (Proposal for a Regulation of the European Parliament and of the Council of the 25.01.2012 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011). On the GDPR proposal, with specific reference to the iconic privacy policy, *see* JS Pettersson, 'A brief evaluation of icons suggested for use in standardized information policies. Referring to the Annex in the first reading of the European Parliament on COM (2012) 0011', WP Universitetstryckeriet Karlstad, 2014. More in general *see* S de Jong, D Spagnuelo, 'Iconified Representations of Privacy Policies: A GDPR Perspective', in Á Rocha, H Adeli, L Reis, et all (eds.), *Trends and Innovations in Information Systems and Technologies* (Springer, 2020).

[18] The difference between express and explicit consent is unclear and it would appear that explicit consent is nothing more than an express consent characterized by greater determination in the behaviour of the user. IA Caggiano, 'Il consenso al trattamento dei dati personali' [2017] DIMT 20 ff.; G Zanfir, 'Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law' (2014) Reloading Data Protection 11.

communication technologies (ICT)[19] from the age of 16 (art. 8 GDPR).[20] However, each dingle Member States can establish a lower age for the processing of minors' personal data (in any case not less than 13), that in Italy it is set at 14 years (art. 2 *quinquies* of the Italian privacy code).[21] Moreover, if the minor is under the established age to give his or her consent, the processing is lawful when such consent is given or authorised by the holder of parental responsibility. More specifically, recital 32 considers as lawful any positive act clearly indicating the willingness of the user to consent to the processing of his or her personal data, such as in the case of the consent provided online. This mode of consent is currently very common with the use of electronic means, such as a smart toy, where are accepted certain actions that appear to be more closely related to implied consent rather than the express consent that does not match the definition of positive act. In this light, in the last year has been clearly highlighted the limits of the current consent to the processing of personal data both because the data subject is unaware of the kind of data processed and the type of data processing carried out in relation to his or her data, and because, even when it is consciously given, it does not prevent a harmful processing for the user, unless accompanied by adequate security protection tools.[22]

Concerning the performance of a contract of which the data subject is a party as a lawful basis (art. 6, para.1, let. b), GDPR).[23] It seems important to underline that these are rather

[19] Precisely art. 8 GDPR refers to the direct offer of the information society services, i.e. those services normally provided for remuneration, at distance, electronically and at the individual request of a recipient of the services, such as social networks and sharing platforms, pursuant to art. 1, directive 2015/1535/EU, expressly mentioned by art. 4 GDPR). The applicability of art. 8 GDPR only to information society services is a main distinction between this European standard and the US one applicable in general to online activities (§312.5 on Parental consent) of the Children's Online Privacy Protection Act of 1998 (so-called COPPA), available at https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5, accessed by 7th December 2020. *See* IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori', in C Fabricatore, A Gemma, G Guizzi, N Rascio, A Scotti (eds), *Liber amicorum per Paolo Pollice* (Giappichelli, 2020), 87.

[20] On minors' consent to the processing of personal data in a digital age, authoritative academic literature has been pronounced. Reference is made to Caggiano for an in-depth analysis of the issue: IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori' (n 19), 87 ff.; IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (n 13), 10 ff..

[21] Italian legislative decree 30 June 2003, no. 196, Code regarding the protection of personal data, containing provisions for the adaptation of national law to Regulation (EU) no. 2016/679 of the European Parliament and of the Council, of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / EC, as at last amended by legislative decree 10 August 2018, no. 101 (Italian privacy code) OJ 174. In Italy, the choice of setting the minimum limit for consent to the processing of personal data at 14 years appeared to be an appropriate choice as it complies with the provisions established for consents relating to other national legislation: adoption law n. 184/1983 and cyberbullying law n. 17/2017.

[22] L. Gatt, R. Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (forthcoming); L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Politica del diritto 350 f.; IA Caggiano, 'Il consenso al trattamento dei dati personali' [2017] DIMT online, 20 ff.; G Zanfir, 'Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law' (2014) Reloading Data Protection 237 ff.. More specifically on the efficacy of minors' data protection law *see* IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori' (n 19), 90 ff..

[23] EDPB, Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, no. 2. IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori' (n 19), 89 ff.; IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (n 13), 14 ff..

limited for two kinds of reasons. First of all, and more generally, this legal basis of the processing refers only to cases in which the processing of data is necessary for the execution of the contract or to take steps at the request of the data subject prior to entering into a contract and does concern only the processing of the personal data strictly necessary for this purpose. Secondly, and more specifically in relation to the processing of minor's personal data, since the data subject is a minor and is lacking his or her capacity to act, the contract should be concluded by the subject in charge of the parental responsibility who would simultaneously authorise the data processing of the minor, but only those processing expressly necessary for the execution of the contract. Obviously, the contracts of the everyday life, of modest value, and not very risky, are an exception, been able to be concluded by the minor (according to authoritative thesis,[24] at least 16 years of age or that established by national law) who contextually agrees to the processing of his personal data (such as contract to purchase a mobile phone number or to by a mobile app).[25]

Last but not least, a possible way to strengthening the *ex ante* remedies of data protection should be the implementation of the principle of privacy by design and by default (art 25, GDPR) and that of security by design by default, the seconds will be analysed in following subparagraph (2.2). These principles are clear examples of techno-regulation: at the time of the determination of the means for processing and at the time of the processing itself, the controller shall implement appropriate technical and organisational measures, which are designed to implement users' privacy and security.[26]

2.2. Smart toys' cyberattacks.

Another very serious and concrete problem relating the IoToys is the possibility that they can be hacked. Concerning cybersecurity and, in particular, the protection of minors from hacker attacks of their smart toys, this risk is strictly connected to the first concerns: how smart toys are connected online, hackers can enter in the smart toys producing personal or property injury.

In particular, cyberattacks imply the hackers can enter in the smart toys' systems producing psychophysical injury or property damages. Among physical injury, very possible are that of data breach, psychological manipulation and personal injury. About property damages, instead, damages to the smart toy or other goods in the surrounding environment, are very serious.

The Fisher-Price 'Smart Toy' could be an example of what the risks involved in smart toys could be, as an effect of cybersecurity issues. The Fisher-Price 'Smart Toy' was one of the first, if not the first, smart toy on the market. The range included three different plush animals - a bear, a monkey and a panda – all connected to the Internet, which worked along with a companion app and smart cards that provided different activities the child could have done with the toy.[27] The toy was able to interact with the children on the base of the command given through an app managed by the parent(s). It was basically a robot but was

---

[24] IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (n 13), 16.

[25] To better analyse the relationship between privacy consent (Art. 6, para 1, lett a), GDPR) and contractual consent (Art. 6, para 1, lett b) GDPR) of the minor *see* IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori' (n 19), 89-90 ff..

[26] For a complete analysis on the principles of data protection and security by design and by default, please see European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018. May me refers to MC Gaeta, Critical issues arising from the Legal Analysis (L.A.)., in L. Gatt, R. Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (n 22).

[27] Fisher-Price described the smart toy as 'an interactive learning friend with all the brains of a computer, without the screen'.*See* https://www.fisher-price.com/en_CA/brands/smarttoy, accessed 3rd December 2020.

equipped with a very basic level of AI,[28] just able to learn some children preferences in order to better interact with him/here. This toy processed personal data and it was a typical example of data-surveillance.

With a tweet dated 22nd July 2019, Mattel (owner of Fisher-Price Company) announced that the 'Smart Toy' was no longer available on the market probably due to different problems that included hiking attacks, which had a huge impact in the public opinion.[29] In fact, already in 2016, it was highlighted some serious vulnerabilities of the so-called Fisher-Price 'Smart Toy',[30] which was analysed at hardware, software, and network levels. Through this analysis, it has been clarified that many of the platform's web service (so-called 'API') calls were not appropriately verifying the 'sender' of messages. This circumstance has strong implications, exposing the smart toy to the risk of cyberattacks, the consequences of which can range from the theft of the minor's personal data to even more. It emerged that the architecture of the smart toy allowed a potential attacker to send requests that should not be authorized under ideal operating conditions. The analysis carried out also highlighted in detail the list of APIs that were found at risk identifying, case by case, the impacts due to each vulnerability.

In particular, it turned out to be possible to find all customers, which provides a list of those customers' toy details and find all children's profiles (identified with name, birthdate, gender, language, which toys they have played with, which purchases have been made). In addition, it seemed also to be possible to create, edit, or delete children's profiles on any customer's account: in the range of the editing activities, it was possible to delete toys, add someone else's toy to a different account) or delete some of the device's built-in functionality. It was also possible to find the status of whether a parent is actively using their associated mobile application or if a child is interacting with their toy at that specific time.

The personal data that an unauthorised person could have stolen would certainly not seem to be sensitive data but, since these are data relating to the personal sphere of children, it is still necessary to pay close attention. First of all, even if the single data may not be relevant in itself, the combination of several data can return a rather detailed profile of the child. Furthermore, the possibilities of modifying the toy or the account linked to the toy, as well as the mere stealing of data, make it clear that the cyberattacks carried out on the smart toy could end up affecting the child.

As it was said, a cyberattack 'could effectively force the toy to perform actions that the child user didn't intend, interfering with normal operation of the device'.[31]That said, it is clear that the smart toy could be used to enable strangers to talk to children through the doll, pushing the child into behaviours that he/she would not otherwise have had, or to make explode the smart toy creating a physical damage for the child. So, the need for straightening the cybersecurity protection it is clear.

---

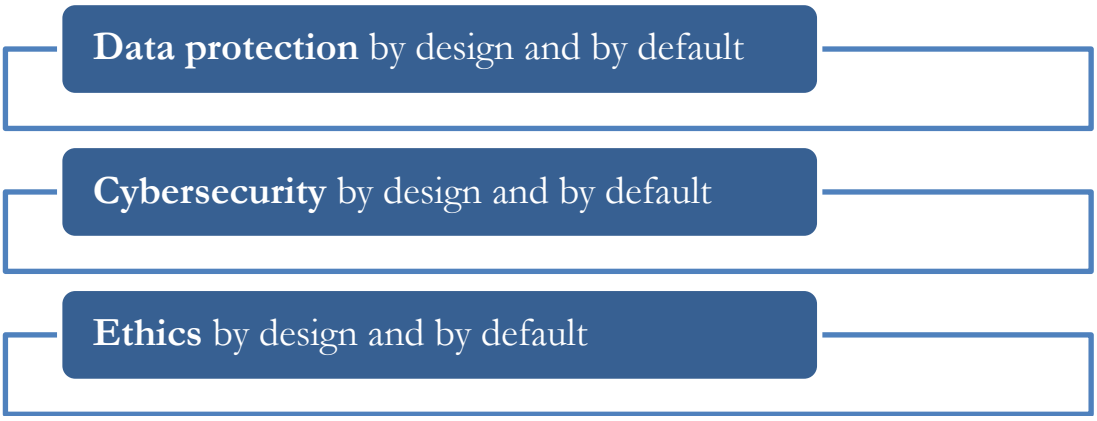
[28] For a definition of AI *see* HLEG, A definition on AI: Main capabilities and Disciplines, 8 April 2019.

[29] *See* D Yadron, 'Fisher-Price smart bear allowed hacking of children's biographical data', available at https://www.theguardian.com/technology/2016/feb/02/fisher-price-mattel-smart-toy-bear-data-hack-technology, accessed 3rd December 2020.

[30] M Stanislav, 'R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy® hereO GPS Platform Vulnerabilities (FIXED)' (2016) Rapid7 Blog, available at https://blog.rapid7.com/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform/, accessed 3rd December 2020. Mark Stanislav was at the time manager for security advisory services at Rapid7. Also *see* R Pinkham, 'API Security Lessons from Fisher-Price's Smart Toy Bear Security Flaw', available at https://smartbear.com/blog/test-and-monitor/fisher-price-smart-toy-data-hackers/, accessed 3rd December 2020. About this analysis, also from a juridical point of view, *see* KL Smith and L Regan Shade, 'Children's digital playgrounds as data assemblages: Problematics of privacy' (2018) Big Data & Society, 2 ff..

[31] M Stanislav, 'R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy®' (n 30).

In order to implement effective preventive protection in the dimension of cybersecurity, certainly, the principles of security by design and by default represents a valid measure. More precisely, in addition to the principles of data protection by design and by default (art. 25, GDPR), that also should be implemented more effectively and efficiently, could be enhanced security measures by design and by default (to which the principle of ethics by design and by default is added, as will be explained inn the following subparagraph). Although not expressly regulated in the GDPR, are however provided in a broad sense in articles 32 and following of the regulation.



The concept of security by design (eg. designing secure hardware, password, PIN, face ID, fingerprint, security key) and by default (eg. installing good antivirus or providing the automatic periodic updating of software) implies that, in addition to the functional requirement, also the design, development and the maintenance of the operative systems must be taken into account to guarantee security (in our case cybersecurity), throughout the life cycle of the operative system. In this direction also the Data Protection Impact Assessment (DPIA), regulated under articles 35 and following of GDPR, can play a very important role in order to evaluate if is it is necessary to implement the cybersecurity measures. In particular, it is useful for the part of the DPIA relating to risks such as offline and online data storage, website and IT channel security, hardware security (including the security key), and measures against malware.

Cybersecurity plays a fundamental role, as data security also implies greater protection of the same data and, therefore, greater privacy of the data subjects. The importance of cybersecurity it is now also known to the legislator, who, although did not intervene properly on security by design by default, however, intervened on the regulation of the so-called essential services characterised by a strong impact of ICT. On this topic, it is worth mentioning that the European legislator in 2016 introduced the so-called NIS directive (Dir. 2016/1148/EU)[32] which aimed to improve national cybersecurity capabilities by preparing member states and requesting them to be adequately equipped. It created European cooperation by setting up a Cooperation Group (art. 11, NIS directive),[33] in order to collaborate at European level and manage cybersecurity risks in all services considered

[32] Directive 2016/1148/EU of the European parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1. The Directive was implemented in Italy by legislative decree 18 May 2018, n. 65 on Implementation of the (EU) NIS Directive.

[33] The Cooperation Group is composed by the representative of the Member State, the Commission and ENISA (art. 11, para 2, NIS Directive).

essential for the economy and the society, strictly related on ICT[34]. In addition, the article 9 of the NIS Directive has also allowed the creation of Computer Security Incident Response Teams (CSIRTs) in each individual Member States that must deal with incidents and risks and ensure effective cooperation at the Union level.[35] After the NIS Directive, the main among the regulation recently adopted for cybersecurity was the Cybersecurity Act (Reg. 2019/881/UE). It consists in a Regulation aimed at creating a European framework for the certification of IT security of ICT products and digital services, and to strengthen the role of the European Union Agency for Cybersecurity (ENISA).[36]

2.3. Ethical issue related to smart toys: from the emotional bonds to the psychological manipulation.

Legal challenges arising from the development of new technologies impose to pay attention on ethical principles. It is undoubtable that ethical principles have the function of integrating and assisting the legal regulation of these phenomena. In particular, with specific regard to smart toys, ethics should strengthen its discipline also endowing it with moral and social values, even intervening before the law, where it appears backward and inadequate.

A recent study of the European Parliamentary Research Service affirms that 'any robot with moving physical parts poses a risk, especially to vulnerable people such as children and the elderly'.[37] This is more and more true in the case of smart toys: in fact, they have very strong ethical implications, due to the possible emotional bonds between the child and the toy.

So, it is not possible to regulate new technologies, and in particular smart toys, without also providing ethical principles (included the principles of ethics by design and by default as an example of techno-regulation) which, in some cases, even precede the introduction of the relevant legal framework. At the same time, it is not possible to provide ethical principles without also binding regulatory principles, which guarantee the certainty of action and its consequences.

It is clear that minors are particularly vulnerable subjects and fall within those categories of vulnerable subjects who can most easily be affected by a bad use of technologies that could lead to an alienation from the real life, or, in the worst cases, could lead to make esteem act that could even lead to the loss of life.

The more recent examples of this terrible problem are the so-called 'Blue Whale'[38] and

---

[34] Concerning the essential services, the figure of operator of the essential service (OSE) has been established. They must take all appropriate and proportionate technical and organizational measures to manage the risks posed to the security of networks and information systems, to prevent and minimize the impact of accidents; they must also notify the incident to the competent NIS authority or the CSIRT.

[35] In Italy, the CSIRT will replace, by merging them, the National CERT (operating at the Ministry of Economic Development -MISE) and the CERT-PA (operating at the Digital Italy Agency - AGID).

[36] All the information on ENISA are available here: www.enisa.europa.eu. At national level, in 2019, the competent NIS Authorities have drawn up guidelines for the risk management and the prevention and mitigation of accidents that have a significant impact on the continuity and provision of essential services.

[37] European Parliamentary Research Service, 'The ethics of artificial intelligence: Issues and initiatives' [2020]. Also *see* V Dignum, 'Ethics in artificial intelligence: introduction to the special issue' (2018) 20 Ethics and Information Technology, 1 ff..

[38] To start Blue Whale you would need to attend forums or groups dedicated to suicide, they usually have names related to whales, and write a message using the hashtag # f57. At that point you would be contacted by a "master" who, it is not known how, would convince the victim that he has personal information that can be used to harm his family. Then the victim has to undergo a series of tests that involve listening to or watching films and songs proposed by the master, self-inflicted injuries or staying for a while on the edge of a very high building or on the tracks of a railway. Obviously, everything must be kept secret, under penalty of death of family members. *See* A Khasawnen, K Chalil Madathil, E Dixon, P Wiśniewski, H Zinzow, R Roth, 'Examining

'Jonathan Galindo'[39] games. Even though are not smart toys, they are both online games where teenagers decide to participate voluntarily following an established procedure. The serious risk of those games is that the teenager could fall into a trap on the web, forced by someone to kill himself, perhaps to save the life of his family or to save himself. The 'Blue Whale' and 'Jonathan Galindo' cases highlight further problematic profiles also in relation to IoToys, even if they are not physical toys but online games.

In fact, if hacking a smart toy is possible, as we have seen in the Hello Barbie and Fisher-Price 'Smart Toy' examples, it could be also possible to talk with the child thought the smart toy, forcing him or her to fall into a trap, exactly as seen on the web with the abovementioned cases. Furthermore, there is the aggravating circumstance that the smart toy is a physical object, with the aspect of an animal or a friend, therefore it can even more easily influence vulnerable subjects such as children. Since the 'Jonathan Galindo' game is even more dangerous than 'Blue Whale', because the unknown person has the aspect of a Disney-like fictional character, an hacked smart toy could be even more dangerous, being a physical 'friend'.

If problems of this type are serious even for boys around eighteen years old, the risk must be taken more seriously with regard to children. Indeed, children do not yet have a well-developed decision-making capacity. In this context, the emotional bonds between children and smart toys could be a serious issue. Therefore, it is necessary that minors, albeit digital natives, are able to understand technologies and their use, as well as distinguish what is human from what is not, without creating emotional relationships with these kinds of toys that are unable to return the feelings.

3. Current regulation for minors' protection as vulnerable subjects in relation to new technologies[40].

3.1. The evolution of the category of personality rights in the digital era.

Coming to this point of the work it is important to focus on the regulation of the individual protection in relation to new technologies, in particular when they are minors. In this line the present subchapter (3.1) will put on the table the personality right and their evolution, while the second subchapter (3.2) will focus on the civil regulation of individuals protection, both in relation to smart product (category that includes smart toys).

The legislator of the second half of the 1900s, after the Second World War, began to move towards the affirmation of values all inspired by the centrality of the individual whose inviolability had to be guaranteed above all other interests and without limitations. Hence the discussion on personality rights initially divided between those who claimed the existence of a single personality right of the individual in all its qualifying manifestations regardless of the single and specific reference legal rule,[41] while others - now prevalent thesis - believed

---

the Self-Harm and Suicide Contagion Effects of the Blue Whale Challenge on YouTube and Twitter: Qualitative Study' (2020) 7 (6) JMIR Ment Health.

[39] *See* D Urietti, 'Cosa sappiamo di Jonathan Galindo' (2020) Corriere della Sera, available at https://www.corriere.it/tecnologia/20_ottobre_01/jonathan-galindo-cosa-sappiamo-sfida-diffusa-online-9ef9beb0-03c1-11eb-84c6-5a6c097a97a1.shtml, accessed 3rd December 2020.

[40] The title refers to the Jean Monnet Chair PROTECH ('European Protection Law of Individuals in Relation to New Technologies') project, co-founded by the Erasmus+ Program (Proposal: Call for Proposals 2019 - EACEA-03-2018; Application number of the project: 611876 -EPP-1-2019-1-IT-EPPJMO-CHAIR), of which Prof. Lucilla Gatt is the chair holder and the author of this contribution is one of the members of the teaching staff. For more information see the website of the project www.protech-jeanmonnet.eu

[41] G Alpa, 'Le persone fisiche (art. 1-10)', in *Il Codice civile*, Commentary Directed by P Schlesinger, G Alpa A Ansaldo (eds), (Giuffrè, 1996); G. Alpa e G Resta, 'Le persone e la famiglia. Le persone fisiche e i diritti della

the existence of many personal rights according to the various provisions of ordinary legislation, all protected under the Italian Constitution, in particular article 2 of the Constitution as an 'open catalog' of these personality rights.[42]

As a matter of fact, the Constitution literarily attributes the character of inviolability only to four rights: personal freedom (Art. 13), of domicile (Art. 14), freedom and secrecy of correspondence (Art. 15), the right to defense (Art. 24, para. 2). Among these inviolable rights expressly guaranteed by the Constitutional Charter, in the case of smart toys, we should consider the right of domicile, understood in a broad sense (online domicile),[43] or the freedom and secrecy of correspondence. These rights, in fact, appear to be involved in a pathological use of smart toys, for example following cyberattacks.

It has been observed that the domicile,[44] the place where human personality develops more than any other, must be protected from external intrusions, since it is elevated to an inviolable area on a par with personal freedom itself.[45] In an era in which the home has, in turn, become a smart home, thanks to domotics development, particular attention must be paid to the protection of the home and its inviolability. This is all the truer when technological innovation leads to the introduction of particularly advanced smart devices such as smart toys, which come into contact with the subjects most exposed to the risk of being influenced: children, in fact, are unlikely to be aware of a greater or lesser intrusion of the smart toy into one's home and personal sphere. It is possible to think, from the hypothesis in which the child authorizes the smart toy (or the same toy is hacked) to take videos[46] of moments of private and personal life that take place within the home, to that of the hacker how may manipulate the child, even reaching to asking him/her to open the front door or commit other inappropriate acts. Makes us reflect also the very concrete cases in which the smart toy processes children's personal data for profiling purposes to improve its AI through machine learning algorithms. From this point of view, therefore, the protection of rights such as that, takes on further facets in light of the introduction of smart devices and in particular smart toys, since these are devices intended to be used by less aware individuals, such as children.

Furthermore, even in the absence of an express wording, it is also known that other rights recognised by the Constitution are also included in the 'open catalogue' of inviolable rights enshrined in Article 2. Thus, for example, the Constitutional Court affirmed that have to be considered inviolable also the right to life,[47] the right to freedom of expression (art. 21),[48] the

---

personalità', I, *Trattato di diritto civile*, directed by R. Sacco (Utet, 2019) 145 ff.; P Rescigno, 'Personalità (Diritti della), *Enc. Giur. Treccani XXVI* (1994)

[42] P Rescigno, 'Personalità (Diritti della) (n 41).

[43] On the new concept of online domicile *see* article 7 of the Commission for Internet rights and duties, Declaration of Internet rights, version after consultation of 14 July 2015, available at https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf, accessed 4th December 2020.

[44] About the freedom of domicile *see* M della Morte, 'Art. 14', in R Bifulco, A Celotto, M Olivetti, *Commentario alla Costituzione* (2006) 1 Torino, 56 ff..

[45] L Vizzoni, 'Dispositivi domotici e dati personali' (n 6), 1032 ff..

[46] In this regard, *see* Italian Constitutional Court, 11th April 2002, no. 135. In this decision, the Italian Constitutional Court addressed the question of the constitutional legitimacy of the visual recordings or video recordings made in the home, raised with reference to Articles 3 and 14 of the Constitution. The decision, in particular, intends home freedom as the "right to protect from external interference, public or private, certain places in which the intimate life of each individual takes place." On this decision, *see* A Pace, 'Le videoregistrazioni 'ambientali' tra gli artt. 14 e 15 Cost.' (2002) Giur. cost., 1070 ff..

[47] Italian Constitutional Court, 15 June 1979, no. 54 and 25 June 1996, no. 223.

[48] Italian Constitutional Court, 24 June 1970, no. 122.

right to health (art. 32),[49] which may be considered of course also as a right to psychological health. Moreover, the Constitutional Court included the rights of the person in the family,[50] the rights relating to the possibility of having a family,[51] the children's rights[52] to education, maintenance and upbringing.[53]

Many of the rights above mentioned, as have been seen, may equally risk being compromised in the event of a pathological use of smart toys. Moreover, as is well known, constitutional jurisprudence now believes that the category of inviolable rights must extend beyond those explicitly or implicitly recognised by the Constitution, giving life to an 'open catalog' of rights,[54] which can therefore also include new generation rights, including those of the personality, born on the occasion of the development of new technologies and the Internet.[55]

The meaning of article 2 of the Constitution would be, according to this now practically peaceful concept, to open the category to new personality rights that arise due to the evolution of society and, therefore, in this case, also due to the development of new technologies.

Concerning privacy, the Italian Constitutional Charter does not expressly provide a privacy right, even if it finds a Constitutional basis, first of all, in article 2,[56] and then in articles 14, 15 and 21. Privacy right has been developed starting from the more general right to respect the private and family life, home and correspondence provided also at international level under article 8 of the European Convention on Human Rights (ECHR)[57] as well as, at European level, under article 7 of the Charter of Fundamental Rights of the European Union.[58] The data protection right, instead, is foreseen by article 8 of the Charter of Fundamental Rights of the European Union and article 16 of the Treaty on the Functioning of the European Union (TFEU), and it is an independent right with respect to the more general right to privacy.[59] As a matter of fact, the protection of personal data is a matter that has always affected society, re-emerging from time to time in different aspects. The terms confidentiality, privacy and data protection are often used as synonyms. While connected, these three are different concepts. Confidentiality can be divided into two aspects: (i) the right to privacy (more precisely is the respect of private life) and (ii) the protection of

---

[49] Italian Constitutional Court, 24 May 1977, no.103 and 5 July 2001, no. 252.
[50] Italian Constitutional Court, 22 December 1982, no. 258.
[51] Italian Constitutional Court, 1 July 1986, no. 199 and 14 July 1976, no. 181.
[52] For a more detailed analysis of children rights, *see* European Union Agency for Fundamental Rights and Council of Europe, Handbook on European law relating to the right of the child, 2015; European Commission, EU acquis and policy documents on the rights of the child, April 2020.
[53] Italian Constitutional Court, 1 July 1986, no. 199 and 23 May 2003, no. 198.
[54] In particular, this approach has been followed by constitutional jurisprudence starting from the judgement Italian Constitutional Court, 10 December 1987, no. 561. The majority literature was already oriented in this direction. *See* A Barbera, 'Art. 2 Cost.', in G Branca (ed), *Commentario alla Costituzione* (1975) Bologna-Roma, 84-85.
[55] *See* TE Frosini, 'Il costituzionalismo nella società tecnologica' (2020) 4 Dir. Inf., 465 ff.; R Romboli, M Labanca, *Il futuro dei diritti fondamentali* (2020) Pisa; A Iannotti della Valle, 'L'età digitale come "età dei diritti": un'utopia ancora possibile?' (2019) 16 Federalismi; TE Frosini, *Liberté Egalité Internet* (2015) Napoli; S Rodotà, *Il diritto di avere diritti* (2012) Roma-Bari; TE Frosini, 'Il diritto costituzionale di accesso a Internet' (2011) 1 Rivista AIC.
[56] Italian Constitutional Court, 4 December 2009, no. 320, according to which the right to privacy belongs to the sphere of protection of art. 2 of the Italian Constitution.
[57] European Convention on Human Rights of 4 November 1950 (ECHR).
[58] Charter of Fundamental Rights of the European Union of 18 December 2000 [2000] OJ C 364/10.
[59] The difference between the right to privacy and data protection is evident in the Charter of Fundamental Rights of the European Union arts 7–8.

personal data, as fundamental right,[60] and as autonomous personality right which is founded on the power of self-determination.[61] Even if data protection constitutes an autonomous personality right, could be considered as a subcategory of the right to privacy, since one of the cases in which the right to privacy is infringed is the abusive processing of personal data.[62]

Lastly, it should be recalled that Convention for the protection of individuals with regard to automatic processing of personal data (so-called Convention 108), firstly adopted by the Council of Europe in 1981 and lastly amended in 2018.[63] It was the first binding international agreement for the signatory States on data protection. In 2018 the Council of Europe updated the Convention 108 in order to address the challenges for privacy resulting from the use of new information and communication technologies as well as to strengthen the convention's follow-up mechanism.

3.2. The civil regulation applicable to smart products.

The meaning that is currently attributed to the rights of the personality is a recent achievement compared to previous frameworks which attributed a public law nature to the entire system of individual protection, limiting the effective protection of the individuals to only the cases of some interpretation of public law rules allowing to take legal action to assert the personality right.[64]

Fortunately, this public law framework for the rights of the individual has been completed by private law rules that made a step forward in the more direct regulation of the protection of the individual, also in relation to new technologies, even if it is only a starting point to be implemented in the optics of a strengthening of effective preventive and remedial protection.

In particular, in addition to the already mentioned GDPR and NIS Directive, it is necessary to consider the Product liability Directive (PLD)[65] and the two Directive sales contracts for goods and digital content.[66]

As a matter of fact, smart toys are product and so are regulated, at European level, by the PLD for all the cases of product defect. In Italy, the PLD was firstly implemented in 1988[67]

---

[60] L Califano, *Privacy: affermazione e pratica di un diritto fondamentale* (ESI 2016); M. Gambini, 'La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela', (2013) 1 Espaço Jurídico, 149 ff.; GF Aiello, 'La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale «disomogeneo» alla luce della nuova proposta di General Data Protection Regulation' (2015) 2 Osservatorio del diritto civile e commerciale, 16 ff.

[61] CM Bianca, FD Busnelli, (eds), *La protezione dei dati personali*, vol 1 (CEDAM 2007) XX ff.; CM Bianca, *Diritto civile*, vol. I, *La norma giuridica. I soggetti*, (2nd edn, Giuffrè, 2002), 180.

[62] On the infringement of the right of privacy *see* M La Pietra, 'Il caso Soraya', in M Bianca, AM Gambino, R Messinetti (eds), *Libertà di manifestazione del pensiero e diritti fondamentali* (Giuffrè 2016), 169 ff..

[63] Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) of 28 January 1981, lastly amended by the 2018. For in-depth Convention 108, see A Mantelero, 'The future of data protection: Gold standard vs. global standard' (2021) Computer Law & Security Review, 1 ff., who considers Convention 108 as a potential global standard, after GDPR that has been described as the gold standard.

[64] P Rescigno, 'Personalità (Diritti della) (n 41).

[65] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L210/29.

[66] Directive 2019/770/EU of the European parliament and of the Council of 20 may 2019 on certain aspects concerning contracts for the supply of digital content and digital services, [2019] OJ L136/1; Directive 2019/771/EU of the European parliament and of the Council of 20 may 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28.

[67] D.P.R., 24 May 1988, n. 224, Implementation of the EEC directive n. 85/374 relating to the approximation of the laws, regulations and administrative provisions of the Member States regarding liability for damage caused by defective products, pursuant to art. 15 of the law of 16 April 1987, n. 183

and then repealed by the Italian Consumer Code (in particular, artt. 114 and following).[68] Actually, the PLD refers to traditional goods and not specifically reference to the so-called 'smart products' has done but, according to the European Commission thesis,[69] PLD can also be applied to these second one, at least until there will not be an *ad hoc* regulatory intervention for the creation of a framework of rules that organically discipline Robotics and AI.

To complete this framework there are the tow European directives, among which the sale of goods Directive (SGD) appears most relevant in particular because it refers also to goods with digital elements, so including also smart toys, regardless of whether the sale takes place physically (in shops), online or, more in general, at distance. However also the digital content Directive (DCD) has its relevance for the protection for consumers that pay for a service or provide personal data in exchange for such service. In particular, the DCD concern data produced and supplied in digital form, for example music o video reproduced online, services for the creation, processing or storage of data in digital form, as cloud storage services, services for the data sharing such as social network and sharing platform, and any durable medium used exclusively as a carrier of digital content as USB or DVD. 'Over the top' interpersonal communication services (OTTs), bundle contracts and the processing of personal data are included within the scope of the DCD directive.

This hard law regulation which, as already underlined, represents an implementation of the legislation applicable to the phenomena involving new technologies but it is not enough for the regulation of the smart product and, in our case, IoToys. From 2017 to date, there have been many non-binding initiatives, along with studies and report, symptomatic of the fact that Institutions have understood the need to regulate robotics and artificial intelligence,[70] but specifically concerning smart toys is the Technical Report of the Joint

---

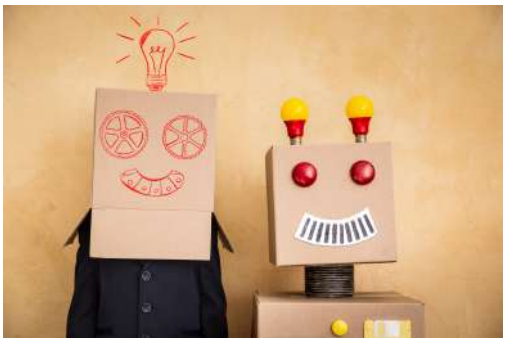
[68] Legislative Decree 6 September 2015, no. 206 (Italian consumer code) OJ 235. To deepen product liability in Italy see A Giorgetti, G Iorio, 'Product Liability (in Italy)', in A Hughes, C Chambers Westgarth, R Freeman, H Lovells (eds), *Product Liability, Jurisdictional comparisons* (European Lawyer, 2014) 215ff..

[69] In 2018 the European Commission has intervened with the last quinquennial report (the fifth for precision, covering the period 2011-2015) on the PLD, which has been complemented by a formal evaluation of the directive. *See* European Commission Report to the European parliament, the Council and the European economic and social committee, of 7 May 2018, on the application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) (COM(2018)246 final). The reporting period is 2011-2017 during which the EU Commission declares that did not receive any complaints or launch any infringement proceedings. At the same time, though, the EU Commission mean PLD does not cover all aspects of product liability. Indeed, there is space for different national approaches (e.g. on systems to settle claims for damages, or on how to bring proof of damage). Completing the quinquennial report European Commission Staff Working Document, of 7 May 2018, on the evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products SWD(2018) 157 final. The evaluation aims to assess the 'functioning and the performance' of the PLD for the period 2000-2016 and it covers the EU-28 Member States.

[70] European initiative in the field of the regulation of robotics and AI, with particular regard to civil law rules, are different: European Parliament, Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)); European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and social committee and the Committee of the regions on Artificial Intelligence for Europe, 25 April 2018, COM(2018) 237 final; European Commission, Communication from the commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated plan on Artificial Intelligence, 7 December 2018, COM(2018) 795 final; European Commission, Report from the Commission to the European parliament, the Council and the European Economic and Social Committee, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, 19 February 2020, COM(2020) 64 final; Study of the European Parliament, Civil liability regime for artificial intelligence, PE 654.178, September 2020; Report from the Expert

Research Centre of the European Commission. The report in-depth safety, security, privacy and societal issues emerging from the use of the Internet of Toys. At the same time, the report underline possible benefits of higher collaboration between research and the Internet Connected Toy Industry in order to make them more trustworthy.

In Italy, the Italian Data Protection Authority has already shown interest on the matter and its risks that have been demonstrated by the informative schedule published on its website.[71] In the schedule, the Italian DPA aims to make aware the community about the functioning and the risks related to smart toys, specifically on data protection and cybersecurity.





Italian Data Protection Authority, Smart Toys: i suggerimenti del Garante per giochi a prova di privacy, 15 October 2018, www.garanteprivacy.it

4. Conclusions: The need for effective preventive and remedial measures.

The straightening of the preventive protection, the enforcement of the duties and of the accountability of the IoToys providers should be implemented. This objective could be realised through the actions of the competent Authorities with their supervisory powers (preventive measures) and, if necessary, imposing high fines (remedial measures), following the way that appears to have been undertaken in recent years. Also, the competent Courts have the power to impose fines and, depending on the case, can be sued as alternatively or in addition to the competent Authorities. Furthermore, it is fundamental the power to orient and positively influence the producers trough soft law (codes of conduct and guidelines),[72] the programmer and the developers.

First of all, it is scientifically proofed that the users do not take necessary attention to the privacy policy and are unaware about the kind of processing of their personal data as well as the kind of data processed.[73] Secondly even when they try to read the policies these appear very difficult to understand. So, more than incentives user to read policies, it should be better to push the producer to respect GDPR principles, writing clear privacy policies and using

Group on Liability and New Technologies, New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies, (Publication Office of the European Union, 2019).

[71] Italian Data Protection Authority, Smart Toys: i suggerimenti del Garante per giochi a prova di privacy, 15 October 2018, available at https://www.garanteprivacy.it/iot/smarttoys, accessed 4th December 2020.

[72] *See* A Iannotti della Valle, 'L'età digitale come "età dei diritti": un'utopia ancora possibile?' (n 55); E Mostacci, La soft law nel sistema delle fonti: uno studio comparato (2008) Milano, 2008; A Somma, 'Soft law sed law: diritto morbido e neocorporativismo nella costruzione dell'Europa dei mercati e nella distruzione dell'Europa dei diritti' (2008) 3 Rivista critica del diritto privato, 437 ff.. May me also refers to MC Gaeta, 'Hard law and soft law on data protection: what a DPO should know to better perform his or her tasks in compliance with the GDPR' (2019) 1 EJPLT

[73] L. Gatt, R. Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (n 22).

effective lawful basis for the processing, as well as to introduce safety standards that the producer has to respect in order to put the product on the market and this security standard has to include privacy and security by design and by default measures.

On the side of the *ex post* protection, of course, the roles and liabilities of the producers of smart toys, the software programmers and apps or platforms developers should be better regulated in terms of high fines for the damages occurred and clear right to clime of the damaged party.

Currently, we can still lean towards an extensive application of existing regulations to the Robotic and AI field. However, to allow a linear and controlled development of Robotics an AI, it is necessary to continue in the direction of the periodic review of current legislation in order to verify its applicability to the new scenario characterised by quick development of new technologies or the need to intervene by modifying it.

Although in part it is still possible to go for an extensive interpretation of the existing rules, in the near future the need to introduce a regulatory framework of rule for Robotics and AI, cannot be ignored. Furthermore, a general law for robotics will not be the solution to regulate the different legal types of Robots and AI.

In general, it is necessary that the ethical principles are reliable (to use the words of European Commission, 'trustworthy'[74]) and place the interests of the individual, as a vulnerable subject in relation to new technologies.[75] Therefore, in some specific sectors, such as smart toys, specific attention to the ethical principles should be given, with the function of integrating and assisting the legal regulation. In fact, as we highlighted, the possible emotional bonds between the minor and the toy, as well as risks of psychical manipulation, need an ethical approach to regulation, which considers these peculiarities.

To sum up, the law should keep up with technologies and evolve with them, in order to assure an effective protection of the vulnerable subject and, in this case, of minors, in the digital habitat or, more precisely, digital playground.

In the digital age, a user experience and human machine interface approaches (UX-HMI)[76]

---

[74] *See* European Commission, Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions: Building Trust in Human-Centric Artificial Intelligence COM(2019) 168 final, according to which: 'Only if AI is developed and used in a way that respects widely-shared ethical values, it can be considered trustworthy'. Also *see* HLEG, European Commission, The assessment list for trustworthy Artificial Intelligence (ALTAI) (2020); European Commission, White paper on Artificial Intelligence - A European approach to excellence and trust COM(2020) 65 final; European Parliament, Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), according to which it is necessary to emphasise 'that socially responsible artificial intelligence, robotics and related technologies have a role to play in contributing to finding solutions that safeguard and promote fundamental rights and values of our society such as […] protection of children'. In Italy *see* AGID, Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino (2018).

[75] *See* UNESCO, First draft of the recommendation on the ethics of artificial intelligence (2020), according to which: 'No human being should be harmed physically, economically, socially, politically, or mentally during any phase of the life cycle of AI systems. […] Persons may interact with AI systems throughout their life cycle and receive assistance from them such as care for vulnerable people, including but not limited to children, older persons, persons with disabilities or the ill'. Also see HLEG, European Commission, Ethics guidelines for trustworthy AI (2019), according to which it is also necessary, considering ethical principles, to 'pay particular attention to situations involving more vulnerable groups such as children, persons with disabilities and others that have historically been disadvantaged or are at risk of exclusion'. For the importance of ethics in regulating robotics *see* L Gatt, 'Per un'intelligenza artificiale antropocentrica. Intervista a Lucilla Gatt' [2020] DIMT, available at https://www.dimt.it/news/intelligenza-artificiale-antropocentrica/, accessed 4th December 2020.

[76] Please, refer to the definitions and the examples contained in the book L. Gatt, R. Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (n 22) which is enterally based on the UX-HMI approach.

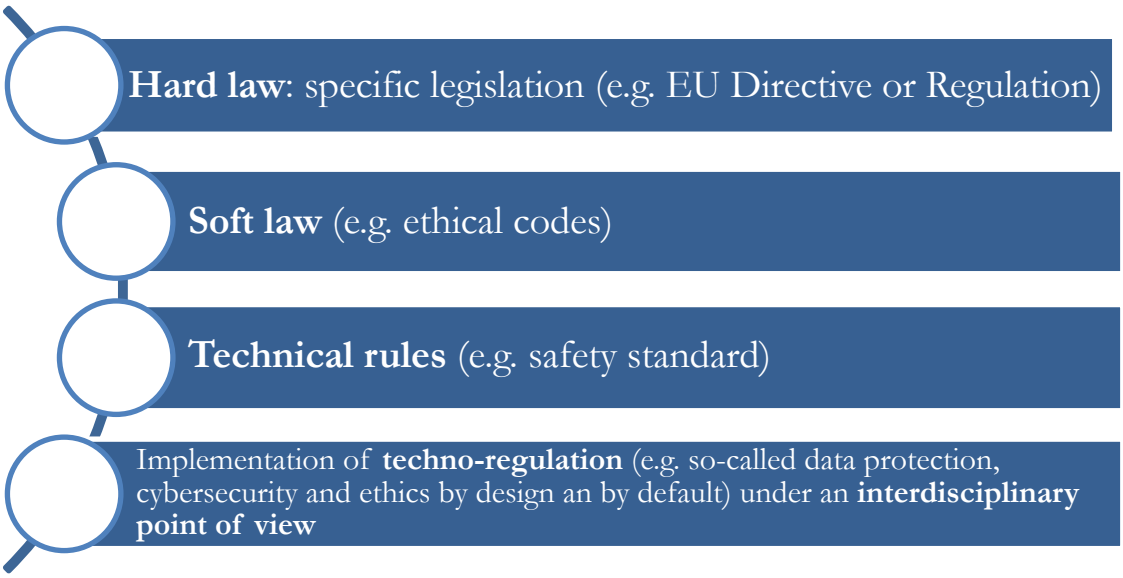
should be considered for measuring the efficacy and the efficiency of the legal rules and for promoting regulations adequate to the aforementioned digital context. In this sense, it is possible to speak not only of legal regulation but of tech-regulation (for example by implementing the principles of privacy, security and ethics by design and by default). The idea of using technologies to regulate technology itself and, in particular, aspects related to the protection of personal data, goes back to art. 17 of the Directive 95/46/EC, that already introduced the technical and organizational measures that the controller should take to protect the personal data. In those years, the Privacy Enhancing Technologies (PET), i.e. technologies to minimise processing of personal data without losing the functionality of an information system, has been developed.[77]

In order to develop techno-regulation, different sciences from the legal one come into play. In fact, nowadays, the level of in-depth analysis required of the new technology law is so high and complex that legal must work in synergy with experts from other sectors of science (e.g. engineers, computer scientists, statisticians, psychologists). As a matter of facts, on one side, legal science needs technical science to understand technologies and provide specific regulations based on its functioning, on the other side, technical science needs the social one for putting in place the principles of techno-regulation based on current law, first of all, hard law, but also soft law, which in this context plays a fundamental role of guidance and orientation.

In the case of the smart toys, which has strong ethical implications, hard law, such as European Directives or Regulations, should be accompanied by soft law, such as ethical codes along with safety standards,[78] to better protect children, as vulnerable subjects, in relation to the risks involved in new technologies.

[77] As usual, California is among the leading Countries in the technology sector and in fact one of the first studies on PETs is from California: I Goldberg, D Wagner, E Brewer, 'Privacy-enhancing technologies for the Internet' (1997) Study of the University of California, Berkeley, https://apps.dtic.mil/dtic/tr/fulltext/u2/a391508.pdf, accessed 24 November 2020. Anonymization technology are included in PET and a first complete definition was provided by A Pfitzmann, M Hansen, Marit, 'A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management' (2010) v0.34, Report of the University of Dresden, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, accessed 24 November 2020. In 2003, then, Borking, Blarkom and Olk reviewed the technologies from a data protection perspective in their Handbook of privacy enhancing technologies. An in-depth analysis is included in the book GW van Blarkom, JJ Borking, JGE Olk (eds), *"PET". Handbook of Privacy and Privacy-Enhancing Technologies. (The Case of Intelligent Software Agents)* (CBP, 2003); J Heurix, P Zimmermann, T Neubauer, S Fen, 'A taxonomy for privacy enhancing technologies' (2015) 53 Computers & Security, 1 ff..

[78] The definition of the standard as part of the soft law is frequent today; however, the standards are technical rules that behaves in very different ways, as to its contents and effects. *See* GM Marenghi *Standard e regolazione condivisa* (Giappichelli 2018), 1ff.


Hard law: specific legislation (e.g. EU Directive or Regulation)
Soft law (e.g. ethical codes)
Technical rules (e.g. safety standard)
Implementation of **techno-regulation** (e.g. so-called data protection, cybersecurity and ethics by design an by default) under an **interdisciplinary point of view**

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Minors' data protection between e-learning and social network platforms

CHIARA SARTORIS
Post-doctoral researcher in Private Law, Department of Legal Sciences, at the University of Florence

Abstract

The paper analyses the impact of Internet on minors' privacy right. It focuses on two aspects. On the one hand, the health emergency of the last few months has imposed schools to provide smart lessons, which, however, pose new problems of data protection. On the other hand, more complex issues are involved when minors use social networks. Thus, it is essential to determine which role parents have and in which extent minors are able to express their consent. The purpose of the paper is to show the new emerging challenges in this field, overcoming some difficulties of coordination between the Italian law and the E.U. framework, in order to assure an effective protection to minors in the digital environment.

Keywords: minor's privacy right - data protection; smart learning; digital consent - social network - compliance.

Summary: Introduction. – 1. Minors and smart learning: new challenges for data protection. – 2. Minors' digital consent in the social network context. – 3. Possible conflicts between minor's digital consent and parents' liability. – Conclusions.

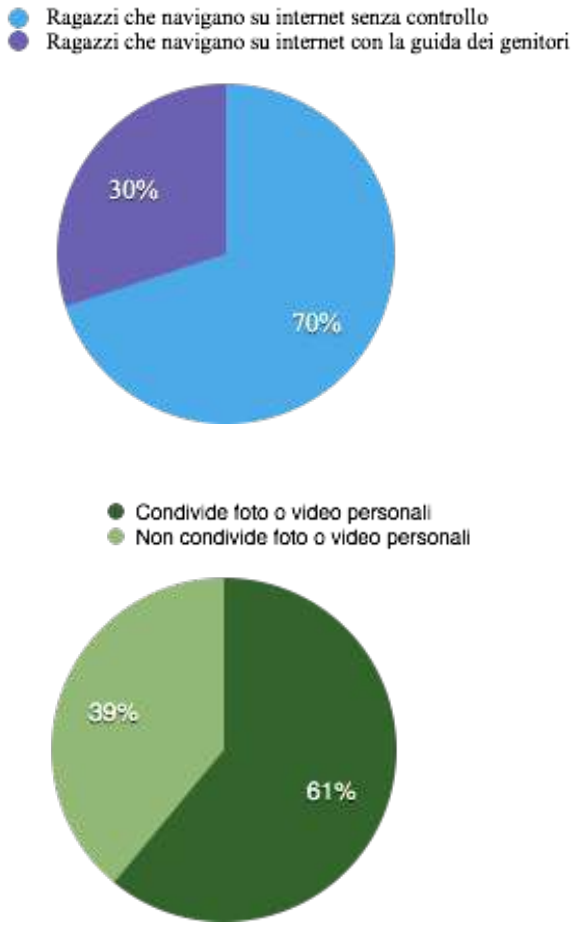
Introduction.

Nowadays, data protection of individuals is one of the most challenging issue from a legal point of view. The development of new technologies and the constant use of the Internet enhance the exchange of personal data in a way which is not always well-informed. The unseen risks of the web may be even more harmful when children are in front of a computer or a mobile phone and are left alone to surf the Internet. Indeed minors may be completely unaware of privacy risks, on the one hand, and may not be able to understand privacy terms of an online service or platform, on the other hand. Such issue has become more compelling in accordance with the increasingly presence of the Internet in children's lives and the amount of time they spend online[1]. Scientific and sociological studies show that the largest percentage of minors use the web to keep in touch with their friends by-means of several social networks, creating their own profile and posting photos or videos with great confidence, but without having any knowledge or – the worst - interest for possible implications about their privacy[2]. Moreover, even adults often use social networks posting

1 See. F Di Ciommo, 'Diritti della personalità tra media tradizionali e avvento di internet', in G Comandè (ed), *Persona e tutele giuridiche* (Giappichelli, 2003); S Livingostone, *Ragazzi online. Crescere con internet nella società digitale* (Vita e pensiero, 2010); A Spangaro, *Minori e mass media: vecchi e nuovi strumenti di tutela* (Ipsoa, 2011); J Van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (Oxford University Press, 2013); S Rodotà, *Il mondo nella rete, quali i diritti e quali i vincoli* (Laterza, 2014); C Perlingieri, 'La tutela dei minori di età nei social network' (2016), Rass. dir. civ., 1324.

2 See. A Thiene, 'L'incosistenza della tutela dei minori nel mondo digitale' (2011), 5, Studium iuris, 528; K Davis, C James, 'Tweens' Conception of Privacy Online: Implicatoions for Educators' (2013), 1, Learning,

photos or videos of their children.



3ª Annual Survey of the Scientific Observatory of the non profit
"Social Warning – Movimento Etico Digitale"
of the 9th February 2021

The problem is that the web is completely transparent and reflects everything we store in it for ever, with scarce possibility to delete the traces of our past. But this is not the worst side of the Internet. The greatest risks for minors are represented by the use that social networks and other platforms can make of personal data they insert in order to access such

Media and Technology, 4; C Perlingieri, *Profili civilistici dei social networks* (Edizioni Scientifiche Italiane, 2014); A Mantelero, 'Teens online and data protection in Europe' (2014), Contr. e impr./Eur., 442; K Montgomery, J Chester, 'Data Protection for Youth in the Digital Age: Developing a Rights-based Global Framework' (2015), 4, Edpl, 277; , K Mc Cullag, 'The general data protection regulation: a partial success for children on social network sites?, in T Bräutigam, S Miettinen (ed), *Data protection, privacy and europea regulation in the digital age* (Unigrafia, 2016), 110; G Spoto, 'Disciplina del consenso e tutela del minore', in S Sica, V D'Antonio and GM Riccio (eds), *La nuova disciplina europea della privacy* (Cedam, 2016), 111; G Pedrazzi, 'Minori e social media: tutela dei dati personali, autoregolamentazione e privacy' (2017), 1-2, Informat. e dir., 437; F Naddeo, 'Il consenso al trattamento dei dati personali del minore' (2018), 1, Dir. informaz. e informat., 27; F Resta, Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione, in GM Riccio, G Scorza and E Belisario (eds), *GDPR e normativa privacy. Commentario* (Wolters Kluwer, 2018), 84; VE Andreola, *Minori e incapaci in Internet* (Edizioni Scientifiche Italiane, 2019); A R Popoli, 'L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato' (2019), 6, Dir. informaz. e informat., 1289; IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori', in C Fabbricatore, A Gemma, C Guizzi, N Rascio, A Scotti (eds.), *Liber Amicorum per Paolo Pollice* (Giappichelli, 2020), 83-100.

services. Thus, from a legal point of view, it is interesting to understand what legal tools can be provided to prevent minors' data profiling when they use social platforms and in which extent adults' behaviours on the web can contribute to breach their privacy. As we will see, the answer can be found partly on the GDPR rules and partly on the Italian civil code rules about capacity and parents' liability.

Furthermore, minors' privacy issues have been meeting new challenges even from another point of view. Within the several problems caused by the COVID-19 emergency, we have to analyse a new area of sensitive privacy. As a result of locked schools, children have been joining lessons on online platforms directly at home from their or their parents' computers or tablets. Such a revolution for the Italian educational system has been implying several problems, especially from a data protection perspective. The use of e-learning platforms by minors and the consequent exchange of data between teachers and pupils by-means of the Internet require to focus on possible privacy breaches to be prevented and to be managed. The positive chances that smart learning will be able to carry out in the next future show the necessity to study also this new aspect of minors' data protection.

On the basis of the above-mentioned considerations, the present study aims at analysing the implication of the Internet on minor's privacy right, focusing on the main rules introduced by the GDPR in the Italian system, with particular regard to both the idea of a minor's right to express her/his digital consent to sign-up on a social platform and the legal role of parents in the use of such platforms. The purpose of the study is to show that the Internet should have a central – and unavoidable – role in the education and the development of new generations. But this challenge requires to guarantee an effective protection[3] for children's privacy by-means of the involvement and cooperation of schools and parents.

1. Minors and smart learning: new challenges for data protection.

In the last few years, the Internet has been assuming a central role in children's education not only for a more frequent use to prepare for a test or to do homework, but also because digital tools are available at school[4]. Italian schools have been experimenting with new educative schemes in which the Internet is a fundamental part. However, in the last months, further privacy problems are emerging when the whole educational activities suddenly have turned into an e-learning school due to the COVID-19 emergency. As a result of the lockdown, schools and teachers had to carry out lessons with the help of new technologies, in particular by-means of the use of either e-mails to exchange didactic materials and

3 To reflect on the importance of the principle of effectiveness see: P Piovani, 'Effettività (principio di)', *Enciclopedia del diritto* XIV (1965), 420; N Trocker, 'Dal giusto processo all'effettività dei rimedi: l' "azione" nell'elaborazione della Corte europea dei diritti dell'uomo (Parte prima)' (2007), 1, Riv. trim. dir. proc. civ., 35; R Oriani, *Il principio di effettività della tutela giurisdizionale* (Editoriale Scientifica, 2008); N Irti, *Significato giuridico dell'effettività* (Editoriale Scientifica, 2009); C Mak, 'Rights and Remedies – Article 47 EUSEE and Effective Judicial Protection in European Private Law Matters', in HW Micklitz (ed.), *Constitutionalization of European Private Law* (Oxford University Press, 2014), 236; G Vettori, 'Contratto giusto e rimedi effettivi' (2015), 1, Pers. e merc., 5.; Id, 'Effettività delle tutele (diritto civile)', *Enciclopedia del diritto*, Ann. X, (2017), 381; Id, 'Il diritto a un rimedio effettivo nel diritto privato europeo' (2017), 1, Pers. e merc., 15 ss.; D Imbruglia, 'Effettività della tutela: una casistica' (2016), 2, Pers. e merc., 62; A Carratta, 'Tecniche di attuazione dei diritti e principio di effettività' (2019), Riv. trim. dir. proc. civ., 1.

4 See. D Valentine, 'Distance learning: Promises, problems and possibilities (2002), 3, Online Jurnal of Distance Learning Administration, 5; M Ingrosso, *Le nuove tecnologie nella Scuola dell'Autonomia: immagini, retoriche, pratiche. Un'indagine in Emilia Romagna* (Franco Angeli, 2004); A Mantelero, 'Adolescenti e privacy nella scuola ai tempi di You Tube' (2011), 2, Nuova giur. civ. comm., 139; K Davis, C James, 'Tweens' Conception of Privacy Online: Implications for Educators' (2013), 2, Learning, Media and Technology, 4; RM Colangelo, 'Istituzioni scolastiche e trattamento online dei dati personali di studenti minorenni (2017), 13, Annali online della Didattica e della Formazione del Docente, 72-89.

homework or online platforms to create virtual classes in which teachers and pupils stay in dialogue and interact simultaneously. As a consequence, parents had to share their personal e-mail accounts with their children or create new ones, as well as to help their children to download applications and to join lessons on e-learning platforms. This situation may potentially disguise some risks for minors' data.

Until this moment, the relationship between privacy problems connected to the Internet and school activities was regarded in a more limited context. For example, minors' privacy protection has come out about photos or videos taken by parents during school plays or about their publication on school websites. But in such cases, it is sufficient for parents to sign their consent for publication. On the contrary, potentially far more complex and dangerous is allowing minors to join smart lessons or to exchange e-mails with their teachers. Consider the possibility that strangers sneak into an e-learning platform in order to acquire student's data or to spread inappropriate contents; or the possibility that students accidentally download virus or malware when trying to access up educational materials sent by e-mail or loaded on the e-learning platform; or, furthermore, they could get in contact with form of surreptitious or fraudulent advertising.

Moreover, unlike other European States, like France, the Italian Ministry for Education has not provided a unique platform to organize smart lessons. Instead, it has only suggested some e-learning platforms to choose between. Thus, each educational institution had to find its own adequate system to carry out lessons. This situation by itself represents a risk for privacy rights. Many service providers have begun to advertise their e-learning platforms, often without offering high levels of privacy protection or – even worse – disguising the risk of data profiling. It is very clear, indeed, that when a platform deals with children, it has to guarantee the maximum standard of security for their personal data, especially when it is selected by a public institution, like a school. The described situation may contrast with both national rules and European and international acts and conventions on privacy matters, that a State has the duty to guarantee with the adoption of effective legal tools.

Apparently, these worries about minors' personal data in the smart-learning environment might sound like a paradox, considering that they are usually free at home to surf up and down the web. But the great difference is that when children are at school, it is the precise legal liability of educational institutions and teachers to guarantee not only their safety and well-being, but also the protection of their rights, including privacy rights. On the basis of these elements, the Italian Privacy Authority, with the Act of 26th March 2020, stressed that schools have to choose e-learning platforms or applications with particular care and with the help of their data protection officer[5]. The choice of a service provider is a key decision and requires particular attention and competence. Thus, according to the Italian Privacy Authority, the selected platform must guarantee both privacy design and privacy by default systems; at the same time, schools have the duty to constantly supervise smart learning activities and to be prepared to immediately adopt effective protection measures even in case of mere suspect of privacy breach[6].

But this is not sufficient. It is also important to focus on the role of the parents. On the

5 The data protection officer's role, in such context, is going to be increasingly important in assuring the respect of privacy law and in suggesting both the best practices to follow for privacy compliance and the best plans to mitigate risks of privacy breach when schools use e-learning platforms.

6 In the note of 17th March 2020 (prot. n. 388), the Ministry of Education had required schools the data protection impact assessment of art. 35 GDPR. But then the Italian Privacy Authority act of 26th March 2020 clarified that the data protection impact assessment is not necessary, unless there are the conditions of art. 35, paragraph 2, GDPR. Thus, such impact assessment is mandatory only when schools deal with the high risks provided by art. 35 GDPR or adopt extremely intrusive platforms, such as those that process biometric data or use geolocation tools.

one hand, parents do not have to give consent to their children's data processing, because schools provide smart learning in the exercise of their institutional functions, according to art. 6, parag. 1, point d), GPRD. On the other hand, however, a complete compliance to the GDPR rules requires that schools show parents the full text of the privacy policy of the selected platform, according to artt. 13-14 GDPR, in order to inform them about several crucial aspects: how to access the system, who can join virtual classes or have contact with children, how didactic contents will be inserted and downloaded, if lessons will be registered and so on. Such information should be provided using a clear and simple language, assuring the transparency of the processing in accordance to art. 12 and the 'whereas' nn. 39 and 58 GDPR. This step, that may appear merely formal and administrative, instead represents a key moment to create a trustworthy relationship between schools, teachers and parents.

On the basis of the Privacy Authority Act of 26th March 2020, the Ministry of Education has recently provided some guidelines that express two other important indications[7]. On the one side, student's data processing can be allowed to the extent that is necessary in relation to the exercise of educational activities, according to the principle of "data minimisation" of art. 5, n. 5, GDPR. On the other side, when a platform provides extra services, schools should select only those tools (virtual class, forum, chat, mail system) that are strictly necessary to carry out lessons and exchange materials and homework. It is also essential that schools do not allow platforms to make data operations, like profiling, which may realize providers' interests not related to smart learning. Consequently, it must be considered illegitimate that a service provider sets conditions for the use of a platform which require the signing of a specific contract or parental consent to data processing for other online services, that are not strictly related to smart learning.

The respect of the described rules and guidelines will certainly contribute to prevent risks for minor's data during smart lessons. It is clear that virtual classes are far from disappearing not only because the health emergency has not completely been overcome yet and may relapse in the next future, but also because e-learning can be a useful instrument, if adequately used and combined with traditional teaching methods. Therefore, schools ought to take up this challenge and, in cooperation with the Ministry of Education, enhance new rules and good practices that assure an effective protection for minors' personal data. A crucial aspect in such evolution is represented by a cultural factor. It is essential that educational institutions and teachers acquire the knowledge of the main privacy rules and privacy policy measures of their schools, with the help of legal and technical experts in this field according to an interdisciplinary approach. Moreover, schools and teachers ought to encourage the relationships with pupils and their parents, providing the letters all the fundamental pieces of information concerning minors' data protection. Against this background, schools have a leading role not only in fulfilling the legal duty to inform parents, giving a transparent view of the adopted privacy rules; but also in contributing to the spread of a "privacy culture" among families with regard to minors' privacy rights: it is essential to develop a new sensibility and to make parents aware of their children's privacy rights. The importance of good practices in the use of the Internet should go hand in hand with the knowledge of the opportunities connected to smart learning. In such way, privacy formation and in-formation provided by schools is a combination that shall become a virtuous circle suitable to enforce minors' privacy protection.

2. Minors' digital consent in the social network context.

7 The note n. 11600 of 3th September 2020 of the Ministry of Education offer guidelines for schools in order to provide some general principles to implement e-learning instruments, with particular attention to security and protection of personal data.

If, as has been said, there are some risks for children's privacy rights in the educational digital environment, there are even greater risks when they surf alone the web. In this context, the access to digital services, like the creation of a social network account, requires user's consent. Thus, it leads to the problem if a minor's digital consent can be considered lawful.

It is common ground that when we create an account on a social platform, we enter into a real contract, which allows us to use the multiple services offered by the provider. It is equally known that such a sign-up implies the consent to our personal data profiling. The disposal of our data is the way we usually pay for the use of a social network. For this reason, contracts should be concluded by users who have the legal capacity to act. Thus, minors should be theoretically excluded form the possibility to have a social network account. Real life, however, shows that things goes very differently because almost every teenager daily uses one or more social networks. That's why it is important to understand how minors can safely and lawfully join such platforms.

In order to analyse this issue, it is important to remember the legal framework of the matter. Nowadays, the GDPR establishes a general framework for national privacy laws of Member States, even with regard to minors' data protection[8]. A key rule in this matter is provided by art. 8 GDPR, which concerns the conditions applicable to child's consent to an information society service, like a social network. The processing of her/his personal data requires the respect of an age limit: on the one hand, the offer of information society services is lawful only if minors are 16 years old; on the other hand, the offer can be considered equally lawful even if minors are below the age of 16, but under the specific condition that consent is given or authorised by the holder of parental responsibility over the child. Such exception, however, cannot be eligible for minors under the age of 13, which represents the minimum limit to respect (art. 8, parag. 2, GDPR).

According to the GDPR, each Member State is able to set a different age limit to express privacy consent, even though most of them reproduce the 13 years-old legal limit determined by the US Federal Law (Children's Online Privacy Protection Act – COPPA)[9], which was the most important benchmark in this matter also for the EU before the GDPR entered into force. This approach can also be explained with the consideration that the main online platforms are based in the USA and, therefore, apply the mentioned COPPA rules. With particular reference to the Italian Law, article 2 of the civil code sets the general 18-years-age limit to acquire the legal capacity to act. But, at the same time, there is a set of rules that seems to recognize minors a "mitigated capacity", *id est* a limited capacity to express consent

8 See. F Pizzetti *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* (Giappichelli, 2016); S Thobani *I requisiti del consenso al trattamento dei dati personali* (Maggioli Editore, 2016); G Finocchiaro *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali* (Zanichelli, 2017); F Piraino, 'Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato' (2017), 2, Nuove leggi civ. comm., 369; IA Caggiano, 'Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali' (2018), 1, Oss. dir. civ. e comm., 81; L Gatt, R Montanari and IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di una riflessione sull'effettività della tutela dei dati personali' (2017), Pol. dir., 363; E Lucchini Guastalla, 'Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori' (2018), Contr. e impr., 106; A Iuliani, 'Note minime in tema di trattamento dei dati personali' (2018), Eur. dir. priv., 293.

9 The Children's Online Privacy Protection Act (COPPA) was passed by the US Congress in 1998 and took effect in 2000 and then was revised in 2011-2013. It regulates the collection of personal information from children under the age of 13 and aims at prohibiting operators of commercial websites or online service platforms or mobile apps from collecting information about children without a verifiable parental consent. The Federal Law has also been enforced by the Federal Trade Commission (FTC), which has the competence for monitoring the compliance to COPPA and for adopting penalties in case of rules breach. Moreover, the FTC states that COPPA applies even to stranger internet providers when their online service addresses also to US children under the age of 13.

for teenagers. There is for example the minor's right to be heard in every issue involving her/him, when she/he is 12 years old (or even when she/he has a lower age and the capacity for discernment) or the minors' right to be heard by a judge within the procedures dedicated to the adoption of decision involving her/his interest[10]. Furthermore, art. 2 *quinquies* d.lgs n. 101/2018 (concerning the compliance of the Italian Law with the GDPR) provides that minors from the age of 14 and beyond can express the consent on their own; on the contrary, beyond the subjective and objective limits of art. 8 GDPR, minors' data processing requires the authorization of the holder of parental responsibility. It is clear that art. 8 of GDPR had a relevant impact on the Italian civil law, because it allows to lower the 18-years-age limit set by art. 2 of the Civil Code. As prestigious scholars observed, the combination of art. 8 of GDPR and art. 2 *quinquies* of d.lgs. 101/2018 seems to introduce a sort of "digital major age", which allows minors to express her/his consent for personal data processing of information digital services[11]. However, it persists a relevant mismatch between the age of 14 capability to express a consent according to art. 8 GDPR and art. 2 *quinquies* d.lgs. n. 101/2018 and the possibility to take legal action in case of breach of her/his rights, since the capacity to act remains acquired at the age of 18. Therefore, from this point of view, the role of parents remains central.

Such considerations require now to be analysed *funditus*. In particular, it is interesting to develop the two following aspects.

First of all, it is important to underline the relationship between the above-mentioned new rules and contract law[12]. It is interesting to understand if and how the breach of art. 8 GDPR may impact contractual validity. On this matter, art. 7, paragraph 4, GDPR states that the *"utmost account shall be taken of whether (…) the performance of a contract (…) is conditional on consent to the processing of personal data that is not necessary for the performance of that contract"*. In order to clarify such rules, the Working Party Article 29 gave a formal opinion called *"Guidelines on consent under the Regulation 2016/679"*[13]: art. 8 GDPR does not concern the problem of validity of contracts between users and providers. Indeed, the contractual legal regime is regulated by Member State laws. This means that a lawful data processing does not necessary imply the validity of the contract. With reference to the Italian law, the question is which contractual remedies can be implemented to protect minors' data, when they express a

10 The above-mentioned laws, introduced by the reform on matter of parent-child in 2012-2013, are the expression of principles stated on international level by the New York Convention of 1989, the Strasbourg Convention of 2003 and the European Union Chart of Fundamental Rights. See: F Ruscello, 'Garanzie fondamentali della persona e ascolto del minore' (2002), Familia, 933; A Gorgoni, 'Capacità di discernimento del minore e incapacità legale nell'adozione' (2011), 1, Pers. e merc., 49-67; Id, *Filiazione e responsabilità genitoriale* (Cedam, 2017); V Di Gregorio, 'L'ascolto, da strumento giudiziale a diritto del minore' (2013), Nuova giur. civ. comm., 2013, 1031; I Bitonti, 'Perenne attualità dell'istituto dell'ascolto del minore' (2017), Riv. Trim. dir. proc. civ., 1069; A Nascosi, 'Nuove direttive sull'ascolto del minore infradodicenne' (2018), Fam. e dir., 2018, 355.

11 See. F Naddeo, 'Il consenso al trattamento dei dati personali del minore' (n 2), 50; A Thiene, 'Riservatezza e autodeterminazione del minore nelle scelte esistenziali' (2017), 2, Fam. e dir., 72; IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori' (n 2), 83; A Astone, 'L'accesso dei minori d'età ai servizi della c.d. società dell'informazione: l'art. 8 del Reg. (UE) 2016/679 e i suoi riflessi sul codice per la protezione dei dati personali' (2019), Contr. e impr., 614; C Irti, Persona minore di età e libertà di autodeterminazione (2019), 3, Giust. civ., 617-650.

12 See. P Rescigno, 'Capacità di agire', *Digesto civ.*, II (1988); G Alpa, 'I contratti del minore. Appunti di diritto comparato' (2004), 5, Contr., 521; M Cinque, 'Il minore e la contrattazione telematica tra esigenze di mercato e necessità di apposite tutele (2007), 2, Nuova giur. civ. comm., 24; M Dogliotti, *'La potestà dei genitori e l'autonomia dei minori'* (Giuffrè, 2007); G Capilli, *La capacità negoziale dei minori. Analisi comparata e prospettiva di riforma* (Giappichelli, 2012); I Garaci, 'La capacità digitale del minore nella società dell'informazione. Riflessioni sul corretto esercizio della responsabilità genitoriale fra esigenze di autonomia e di protezione' (2019), Nuovo dir. civ., 59.

13 Opinion n. 259 of 10th April 2018.

consent beyond the legal limits. The answer in not simple. From a certain point of view, it can be supposed that a contract lacking necessary consent is to be considered void for reasons of an illicit object or the breach of an imperative law (art. 1418 c.c.). But such an approach consequently arises the issue of the effects of a consent expressed by the user in a second moment, since it is debated if a contractual nullity is suitable for emendation. From another point of view, it can be supposed that the sign-up for a social network remains without effect until the expression of the consent is in accordance with the law. So the debate is still ongoing and it will be interesting to analyse the judges' approach with particular reference to the discipline of invalidity of art. 1425 c.c., which seems to be suitable for protecting minors' interest in contractual field[14].

Secondly, it is important to highlight the risk that minors at the age of 14 try to bypass privacy protection rules in order to sign-up for a social network. As has been said, it is a common ground experience of daily life that minors often surf the Internet alone, without paying attention to their privacy rights. Beyond the cultural and technical aspects of the problem, the reality is that children often declare a false date of birth to activate their presence on a social platform; they modify or unsubscribe the original parental authorization, in order to have access to other services offered by the same provider; or they create false profile pages. The described behaviours direct the focus of attention to two aspects: on the one hand, the role of parents is crucial in monitoring their children's behaviour; on the other hand, it is necessary to implement technical and legal measures that social platforms are expected to set up in order to verify the age of their users.

However there is something more to consider.

3. Possible conflicts between minors' digital consent and parents' liability.

It is important to underline another relevant interpretative issue. It was already shown how crucial it is that modern laws recognize minors when they exercise their non-patrimonial rights. At the same time, this approach means that their individual accountability is increasing in many fields, such as in the area of privacy. This situation, however, could create new occasions of conflicts even between minors and their parents. Consider, for example, the possibility that a teenager above the age of 14 expresses her/his consent to the sign-up for a social network or post some photos or video on a platform in contrast to her/his parents' specific will. According to a strict interpretation of art. 8 GDPR and to what as has been said before, it seems that the minor's consent is sufficient to legally access a social platform and to operate on it.

Recognizing an area of autonomy for minors in the digital environment does not mean that parents can give up their legal and educational role. At the same time, laws concerning minors' rights do not imply that parents have no power of decision anymore. On the contrary, parental liability persists even if the child is 14 years old, especially when she/he are online[15]. Parents have the unavoidable duty to monitor and provide assistance to their

14 See V Zeno-Zencovich, 'Profili negoziali degli attributi della personalità' (1993), Dir. inf., 545; G Vettori, 'Privacy e diritti dell'interessato' (1998), 4-5, Resp. civ. e prev., 885; S Viciani, 'Strategie contrattuali del consenso al trattamento dei dati personali' (1999), Riv. crit. dir. priv., 159-190; G Resta, *Autonomia privata e diritti della personalità* (Jovene, 2005); R Caterina, 'Cyberspazio, social network e teoria generale del contratto' (2011), Aida, 96; S Thobani, *I requisiti del consenso al trattamento dei dati personali* (n 8), 89; V Ricciuto, 'I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato, in N Zorzi, F Galgano (eds.), *Persona e mercato dei dati, riflessioni sul GDPR* (Cedam Wolters Kluver, 2019), 95; F Bravo, 'Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto' (2019), Contr. e impr., 34.

15 See V Corriero, 'Privacy del minore e potestà dei genitori' (2004), 4, Rass. dir. civ., 1011; A Gorgoni, *Filiazione e responsabilità genitoriale* (n 9); S Peron, 'Sul divieto di diffusione sui social network delle fotografie e di

children in order to assure that they can express their identity and personality in a safe context with reference to their fundamental rights, like privacy rights. In this perspective, "minor's interest to her/his correct and balanced psychophysical development" provided by several law and acts[16] represents a general limit to the extent of the lawfulness of her/his digital consent. Privacy protection cannot be considered a value itself, especially when it concerns minors: it appears as an instrument to protect other rights, in particular minors' interest to a balanced development. Thus, if parents are expected to interfere each time with their children's actions within the digital environment it may harm such interest. This interpretative approach seems to be the best way to guarantee that minors' consent with reference to their data does not become a mere administrative formality. Otherwise, the protection of those rights would be completely compromised, in contrast to the GDRP principles.

Therefore, the criterion of "the best interest of the child" should be applied by judges in the equally frequent cases in which parents are in conflict among themselves. This situation happens, for example, when one parent does not agree with the decision of the other to post personal data (photos or videos) concerning their child on a social platform, in case the child is still under the age of 14 (the so called "sharenting" phenomenon)[17]. The combined interpretation of artt. 316 and 337 *ter* c.c. provides that each decision concerning children (including those regarding their privacy rights), ought to be taken with the consent of both parents and, in its absence, with a tutelary judge's authorization. The parental conflict can be overcome only with reference to the child' s best interest. That is the reason why, according to several national and international rules, judges have to hear the child, due to her/his right to be heard within the procedures and the decisions in which she/he is involved.

Conclusions.

The above-mentioned considerations highlight that minors' data protection today represents a central issue for the agenda of each State. The present health emergency has been having a catalytic role for a series of problems concerning minors' privacy rights, that require to be solved. The launch of digital classes on online platforms is the last evidence of the increasing importance of the Internet in the education and development of our children in a word which is getting more and more interconnected. Therefore, it is important that minors are able to adequately use new technologies and, at the same time, benefit from their

altri dati personali dei figli' (2018), 2, Resp. civ. e prev., 589; M Nitti, 'La pubblicazione di foto di minori sui social network tra tutela della riservatezza e individuazione dei confini della responsabilità genitoriale? (2018), Fam. e dir., 380; C Camardi, 'Relazione di filiazione e privacy. Brevi note sull'autodeterminazione del minore? (2018), 6, Jus civile, 831; G Cassano, 'La responsabilità genitoriale nell'uso dell'odierna tecnologia telematica' (2020), 6, Fam. e dir., 631.

16 In particular, art. 3, par. 1, New York Convention on the Rights of Child; art. 24, par. 2, Charter of Fundamental Rights of the European Union; artt. 316, 317 bis, 321 c.c.; artt. 11, 25, 57 legge n. 184/1983. See the following studies: S Parker, 'The best interests of the child. Principles and problems', in P Alston (ed), *The best interests of the child. Reconciling culture and human rights* (Clarendon Press, 1991), 26; S Arbia, 'La Convenzione ONU sui diritti del minore' (1992), in Dir. uomo, 39; F Santosuosso, 'Il minore e la garanzia dei diritti inviolabili dell'uomo' (1997), Iust., 361; P Ronfani, 'L'interesse del minore: dato assiomatico o nozione magica?' (1997), 1, Soc. dir., 47; C Focarelli, 'La Convenzione di New York sui diritti del fanciullo e il concetto di «best interests of the child»' (2010), 4, Riv. dir. int., 981; P Martinelli, J Moyerson, 'L'interesse del minore: proviamo a ripensarlo davvero' (2011), Min. giust., 7; R Rivello, 'L'interesse del minore fra diritto internazionale e multiculturalità', (2011), Min. giust., 15.

17 See D Cino, S Demozzi, 'Figli "in vetrina". Il fenomeno dello sharenting in un'indagine esplorativa' (2017), 2, Riv. it. edu. fam., 153-184; SB Steinberg, 'Sharenting: Children's Privacy In The Age Of Social Media (2017), 66, Emory Law Journal, 839-1007; G Bonanomi, *'Sharenting. Genitori e rischi della sovraesposizione dei figli online'* (Mondadori, 2020); M Foglia, 'L'identità personale nell'era della comunicazione digitale, in F Bilotta, F Raimondi, *Il soggetto di diritto. Storia ed evoluzione di un concetto nel diritto privato* (Jovene Editore, 2020), 265-276.

infinite opportunities. However, our legal system should provide a set of effective tools to protect minors' privacy rights in the digital environment, in accordance with European rules and principles.

Such a purpose can be reached by-means of cooperation and actions on several levels based on an interdisciplinary approach.

With reference to smart learning, firstly, the use the Internet is a challenge that the Italian system cannot ignore. It requires, however, a great attention from two points of view: on the one hand, educational institutions have to make their teachers aware of the problems connected with the use of smart learning systems, providing them a specific education in terms of either computer skills or privacy law. On the other hand, school directors and educational data officers have to draft adequate privacy policies to be submitted to parents, taking into account the new aspects of data protection regarding smart learning. The formative and in-formative moment are crucial aspects.

Secondly, parents maintain a central role with reference to their children's use of the Internet outside school-time. The new personality rights that recent Italian, European and International acts recognize are contributing to a new approach to minors' self-determination in several fields. This draws the attention of scholars and jurisprudence to read the rules of the Civil Code about the capacity to act through different eyes, reflecting upon the possibility that minors are able to enter into contracts concerning their non-patrimonial rights. However, this does not means that parents are exempted from their obligations. From this particular point of view, the more minors acquire a larger capacity to express their consent in the digital area, the more parents have a significant duty to monitor their online activities and behaviours, under the liability of parental authority according to art. 316 c.c.. The "minor's interest to her/his correct and balanced psychophysical development" represents the limit of minors' self-determination also in the digital context.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Distance teaching in times of Covid-19 – from zero to hero?

Experiences and best practices of a university lecturer trying to create a student-centred distance teaching approach

ARNDT KÜNNECKE
Professor at the Federal University of Applied Sciences for Public Administration of Brühl

Abstract

This article deals with the challenges of distance teaching during the Covid-19-induced global pandemic. As hardly any university teacher was prepared for switching from traditional in-class teaching to distance teaching, and as most universities were neither personally nor technically equipped for such a dramatic change, nearly everybody had to start from zero. As a university teacher in Germany, I devised my own student-centred method of distance teaching, combining various available means and tools for distance teaching and learning, which include: Videos, WhatsApp and Zoom (VWZ). The VWZ-approach turned out to be a very promising and effective method of distance teaching and learning. It puts the students in the centre and gives them better control over their study and learning process at anytime, anywhere, and according to their own learning speed, while the teacher is constantly available for them to provide guidance, answer questions and give them feedback.

Keywords: Covid-19 - Distance Teaching - Virtual Classroom - Flipped Classroom - Learning Platform - ILIAS - BigBlueButton - Blackboard Collaborate - VWZ-approach - Video - WhatsApp - Zoom

Summary: Introduction. – 1. Starting off from zero. – 2. Failed attempts: Virtual classroom lectures. – 3. Best practice: VWZ-teaching. – 4. Advantages of the VWZ distance teaching approach. – Conclusions.

Introduction.

On 13th March 2020 my colleagues and I received an e-mail from our university, indicating that the university would be closed from the 16th March due to the restrictive measures in Germany because of the Covid-19 pandemic. We were asked to get in touch with our students via e-mail or the university's learning platform and provide them with some material and tasks for the forthcoming two weeks. During that time, we would receive more detailed instructions on how to provide distance teaching during the closure of the university.

This short e-mail made the scheduled and planned work for face-to-face teaching in the forthcoming weeks completely obsolete, and we all had to switch on to online teaching. Did the university provide us with any help or assistance? Was anybody prepared for this sudden and drastic change? No! We all had to start from zero. Maybe not to become a hero of distance teaching immediately, but at least to provide some decent distance teaching in the near future. This essay will examine the challenges and difficulties posed by the sudden switch to online distance learning and how we tried to overcome them.

1. Starting off from zero.

As a university lecturer in law and political science I have been teaching at various universities for more than a decade, I was used to face-to-face teaching in classrooms and auditoriums. This was also the part of the job I enjoyed most: being together with the students in a room and teaching them subjects in an interactive, colourful and entertaining way. For this way of teaching I had passion, was experienced and prepared. But now the university was closed, and the face-to-face contact with students was also over. So, what should I do?

The first week of the Covid-19 lockdown was still easy to handle somehow, as it was my last week of lectures in a couple of courses in which students were about to take their final examinations. Having finished my teaching prior to university closure, I e-mailed the students tasks and exercises in preparation for the examinations. I also ensured that I was available to answer questions and provide feedback via the university's e-mail system. However, the greatest challenge was delivering six new courses on German Constitutional Law, EU Law, German Foreign Policy and Public International Law a week after the university closed down for face-to-face teaching.

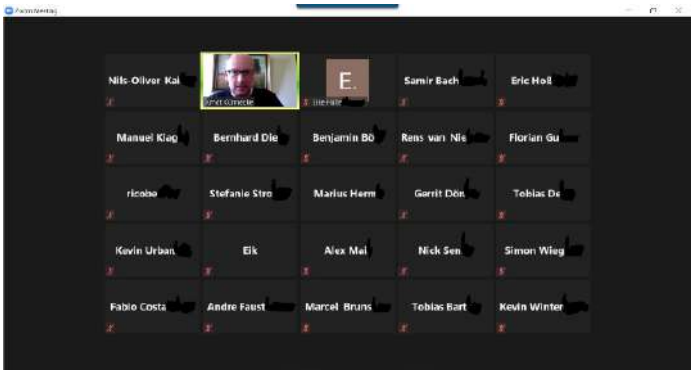
In the meantime, my university instructed the lecturers to prepare for online distance teaching in accordance with the original timetable scheduled for face-to-face teaching until the end of April. The university's main concern was obviously to ensure that all lecturers were actually working. Therefore, we were supposed to welcome the students via e-mail at the beginning of each scheduled lesson, give them teaching materials, assign tasks and be available online to provide feedback to students via e-mail or on the university's learning platform *ILIAS*[1]. My main concern with online teaching was the inherent challenge of how to replicate lecturer/student familiarity and intimacy that face-to-face teaching afforded, within the online environment?

My first idea was to schedule all classes in a virtual classroom. Some years ago, I had gained some experience with the online cloud meeting platform *Zoom*, which is a web-based video conferencing tool with a local, desktop client and a mobile app that allows users to meet online, with or without video.[2] Users can choose to record sessions, collaborate on projects, and share or annotate on one another's screens. This simplified video conferencing and messaging tool encompassed all technical features that are important for a virtual classroom. Especially, key features like video, audio, chat and the screen-sharing function provided all the necessary tools for online teaching. However, while sharing a presentation using the screen-sharing mode, it was only possible to see a maximum of four participants at the same time on a small video screen next to the shared presentation. The rest of the participants were not visible at once.



[1] For more details about *ILIAS* see: https://www.ilias.de/en/.
[2] For more details about *Zoom* see: https://zoom.us/meetings.

You had to scroll down to see the next couple of them. This feature was only suited to teaching a small group of 3-5 students, while all of them were using video. However, in bigger groups it meant that the great majority of participants was hidden. This could only be avoided by not sharing the screen.



But as I intended to use my normal presentations designed for face-to-face teaching, I had to share my presentations with the students. Therefore, I dropped the idea of using *Zoom* online meetings as the main tool for distance teaching. For me as a teacher, it is essential to see my students to ensure that they understand my teaching. In-class teaching allows for real time feedback partly by watching students' faces. If this feedback does not exist, it makes me feel disconnected from the students without the ability to understand their level of engagement or understanding of the lecture. It also feels like talking to my computer screen for many hours each day without knowing if the students understand the lecture or are fully engaged with the teaching. Having no visual contact with the people you teach online means that you do not even know if they are still physically present in front of their devices. It makes it possible for lazy students to just log on and fake their attendance when they are not actually engaged with the teaching material. This is what I was told by a couple of students. I also wanted to avoid making a fool of myself lecturing in a virtual classroom where in the worst-case scenario, only a few of the students who logged on were actually listening to me.

2. Failed attempts: Virtual classroom lectures.

Nevertheless, later during the Covid-19 lockdown, I had to practise some online teaching in different virtual classrooms, because the universities where I had additional teaching assignments required me to do so. I realised through these experiences that the current technical platforms for online teaching are inadequate for proper and effective distance teaching.

a) *BigBlueButton* – University of Applied Sciences for Public Administration (Brühl / Germany).

At the end of March, my home university proudly announced via e-mail that a video conference system, called *BigBlueButton*, was being integrated into our university's learning platform *ILIAS*. *BigBlueButton* is an online tool, which enables teachers to share audio, slides, chat, video, and desktop with students. It also offers built-in breakout rooms, polling and recording lectures for later review.[3]

As I was facing the first lecture in a course of 88 actual distance students in the area of

[3] For more details about *BigBlueButton* see: https://bigbluebutton.org/.

EU Law which was supposed to be held as the course introduction face-to-face at university, I wanted to make use of the advantages of the new university owned virtual classroom. My plan was to prepare the whole setting in a classroom at university: computer, smart board, camera, microphone, loudspeaker. I wanted to place myself in the students' real classroom at university next to a smart board on which I could do my presentation. Via camera and microphone, they could see and hear me at home on their own devices and vice versa I could see them on my computer screen and hear them on my loudspeakers. To make sure that the whole system worked, I made a test of the technical equipment the day before the lecture at university with some colleagues from the university's IT department. During the test, everything worked out well. On the following day, at 8 a.m. I started my video lecture on *BigBlueButton*. However, the students could not use their cameras because of poor internet connectivity and low bandwidth servers. The video transmission worked quite well for about 15-20 minutes. After that, I received lots of messages in the *ILIAS* learning platform's chat that the video was frozen and that the students could not hear me properly anymore. So, I switched off my video and tried to talk to the students only via audio while sharing my screen at the same time, showing them my presentation slides. However, after a few minutes I again received messages in the chat that the students could only understand every second or third sentence I said. That made me stop the screen sharing and made me just talk with the students via audio. However, after a short while I received messages in the chat again complaining that my voice did not come through properly anymore. When I tried to respond to the students in the chat, I was wondering why my message just being typed did not appear in the chat. Only five minutes later, my message appeared in the chat, while lots of messages from the students popped up in the chat which were written a couple of minutes before. I realised even the chat had a delay of 12 (!) minutes. That made me quit the lesson. Distance teaching like that was just not possible.

b) *Blackboard Collaborate* – MEF University (Istanbul / Turkey).

Still in March, I had to give three lectures in a course about German Law at MEF University in Istanbul. Originally, these lectures were also supposed to be held in person in Istanbul. For this course with altogether 60 students the university provided virtual classroom facilities on their university owned *Blackboard Learning* platform, called *Blackboard Collaborate*. *Blackboard Collaborate* is an online platform for delivering online courses and meetings in which robust teaching and learning tools such as an interactive whiteboard, multi-point video, and application and desktop sharing can be used.[4] When I started the lecture for my Turkish students, sitting in front of my computer in Germany, while they listened in Turkey, I had my video switched on and tried to share my screen with my presentation. The students immediately wrote me in the built-in chat that they could not hear me at all. However, I could hear their voices when they were talking. So, I switched off the video and tried to deliver my lecture just by using audio and screen sharing. However, again I received messages in the chat that still nobody could hear me. The students were only able to hear me after I stopped the screen sharing mode. They told me that they already had a couple of other lectures being delivered on the same platform, but that they did not face any technical problems with any of their other teachers. Again, it seemed that my internet connection in Germany was not fast and stable enough to successfully participate in an online meeting with a few dozen students. Just being able to talk but not being able to show anything to the students. I had to quit the lesson. Effective distance teaching was not possible this way. The forthcoming lessons I sent them my presentation before class time and explained

[4] For more details about *Blackboard Collaborate* see: https://www.blackboard.com/resources/about-blackboard-collaborate.

it only via audio while each student had to follow the slides being sent before on their computer. This way of distance teaching was also far from being satisfactory to anybody.

c) *Zoom* - V. N. Karazin National University (Kharkiv / Ukraine).

In April I had to give a couple of online lectures about EU Foreign Policy at V. N. Karazin University in Kharkiv. These lectures were part of a Jean-Monnet-Program and they were originally supposed to be held in person in Kharkiv. As the university did not have any virtual classroom tools being incorporated in their university's learning platform, I was asked to hold the lectures on *Zoom*.[5] In comparison to the other lectures I held online, the number of participating students here was much lower, just about 15. As some of the Ukrainian students had no sufficient knowledge of English language, a Ukrainian colleague was translating my lecture consecutively. The translator, one of the students and I used video, the other students did not. While I was lecturing, I was sharing my screen so that the other participants could see my presentation slides and the translating colleague had some written reference for her translation. Technically, everything went well: no problems with video, audio or screen-sharing. However, I had no idea if the students who did not use video could follow and understand what I had explained, or what my Ukrainian colleague had translated. That was very irritating for me as I did not get any feedback during the whole lecture apart from questions being asked by the only student using video who had a good knowledge of English. He was also the only one who tried to answer the questions I posed. This made me feel like lecturing just to two people (the participants with enabled video). The other participants did not say anything during the lecture, so that I had no idea if they were still physically present in front of their devices or if they only stayed logged on while doing something else. These issues made me feel very uncomfortable throughout the lecture.

3. Best practice: VWZ-teaching.

As I was not satisfied with any of these solely virtual classroom-based distance teaching models, I decided to create my own approach. This approach is based on my experiences of teaching according to the *Flipped Classroom* approach. It combines introductory videos being taken from the *Flipped Classroom*, *WhatsApp* as quick and comfortable communication channel and *Zoom* as online meeting platform for face-to-face consultation hours. **V**ideo + **W**hatsApp + **Z**oom = **VWZ**.



V = Video introduction.

The idea to provide an introductory video for each lesson is derived from the *Flipped Classroom* teaching method. The *Flipped Classroom* generally provides a pre-recorded introductory lecture (video and/or audio) which is followed by some in-class activities. The

[5] See: n 1.

students watch and/or listen to this pre-class lecture somewhere outside the classroom and in time before the class starts. When they come to class, they are already equipped with some basic knowledge about the topic of the class so that the freed in-class time can be used for interactive tasks, such as exercises, discussions, Q&A sessions or other learning activities.[6] Flipping the classroom in this sense means changing the process of traditional teaching: instead of introducing the students to the topic physically in class and giving them follow-up tasks for home, the teacher already gives them a pre-class introduction and builds on that basic knowledge to guide the students through learning activities in class which helps them getting a deeper understanding of the topic. In short, taking into account the technical means being used for its realisation, *Flipped Classroom* can be defined as "*any teaching model which replaces in-class lecture modules with video or audio lectures with the goal to use the freed in-class time for interactivity*"[7].

The core feature of the pre-class activities of the *Flipped Classroom* teaching approach are the introductory videos/audios. In comparison to audios, videos have the big advantage that they appeal to more senses than just audio. As some students prefer reading, some listening and some others watching, videos include all three of these learning preferences: they offer text and pictures for the visual needs and sound and speech for the audio needs. So, the audio-visual content of videos serves the different needs of students more comprehensively than only audio or visual content. And it gives the teacher many more means to deliver his/her content. Therefore, as in the *Flipped Classroom*, I chose videos as a central feature of my own distance learning approach.

In law classes, the introductory video to a lesson needs to understandably introduce a legal term, concept, problem or case in short. Ideally, the big idea of the lesson should be included in the video, easy to understand and to remember for each student. The way I do it is mainly by producing an introductory video of 5-15 minutes in length for each lesson. In this video I start with defining the learning objectives, shortly explain the core concept and content of the lesson, emphasizing essential points which should be marked in legal texts or kept in mind, and finally give the students some assignments for their individual space at home. To provide the students a clear and recurring typical structure of each lesson, each video is divided into three parts: (1) learning objectives, (2) key content and (3) assignments.

For the learning objectives it is important to give the students some clear guidance through the lesson and make them focus on what they should have learnt by the end of the lesson. The key content needs to be explained in a clear and precise way, as there is not enough time in a video to provide the content of the whole lesson. It is also important to give the students some useful hints and leads on how to understand and remember the most important parts of the explained topic. This includes directing their attention to key words or paragraphs of legal texts and concepts, to tell them which words of legal texts to mark or underline, to visualise legal concepts, to connect newly introduced content with students' prior knowledge in other areas, or to provide them with some mnemonic tricks to remember

---

[6] Compare Centre for Academic Development and Quality, Nottingham Trent University, *CADQ Guide – The Flipped Classroom* (June 2013) < https://www4.ntu.ac.uk/adq/document_uploads/teaching/154084.pdf > accessed 23 June 2020; LE Davis / MA Neary / SE Vaughn, 'Teaching Advanced Legal Research in a Flipped Classroom' (2013) 22 Perspectives: Teaching Legal Research and Writing 1, 13; Educause Learning Initiative, *7 Things you should know about Flipped Classrooms* <http://net.educause.edu/ir/library/pdf/eli7081.pdf> accessed 23 June 2020; J Lihosit / J Larrington, 'Flipping the Legal Research Classroom' (2013) 22 Perspectives: Teaching Legal Research and Writing 1, 1; WR Slomanson, 'Blended Classroom: A Flipped Classroom Experiment at the Lectern' (2014-15) 64 Journal of Legal Education, 95; A Upchurch, 'Optimizing the Law School Classroom through the 'Flipped' Classroom Model' (2013) The Law Teacher, 1.

[7] L-C Wolff / J Chan, *Flipped Classrooms for Legal Education* (Springer 2016) 13.

the topic more readily.

It is important to mention that the recordings should not be too long, and they should not try to replace the whole lecture. This material is only the introductory part of the lesson. Evaluations showed that the attention span of the students watching and/or listening to content delivered online is restricted to maximum 15-20 min.[8] Keeping the video short and to the point – that is the key to keep the student's attention.

In general, for producing pre-class videos, there are three main ways: the 'screen capture approach', the 'white board approach' and the 'green screen approach'. In the screen capture approach, the teacher creates a visual presentation, such as PowerPoint, Pdf or a Word document, and records his or her voice while showing and running the presentation or document on the computer. The video then shows the movement of the presentation or document on the computer screen synced with the recorded audio of the teacher.[9] For this kind of recording, screen capture software such as *Camtasia*[10] or *Snagit*[11], are quite easy to handle and can be used. In contrast in the white board approach, the teacher films him- or herself in front of a white board, flip chart or screen.[12] In the green screen approach, the teacher records him- or herself in front of a green screen. The advantage of the screen capture is that a PowerPoint slide show and the audio recording can be played simultaneously on the students' device, serving both visual and auditory learning styles. In addition, it is relatively easy to update certain parts of the recording, just by changing some slides and re-recording the related audio part.[13] This is rather difficult in the white board and green screen approach. Even for updating a small part of the content, the entire video has to be re-recorded, unless the teacher could appear in front of the camera again in the exact same style and outfit as in the original video. Inserting an update with a teacher looking different to the appearance in the original video would make the whole video look unprofessional and not convincing. Therefore, to avoid needless updates, it is strongly recommended to avoid any unnecessary update references, for example to the names of people holding a specific office, as they can change, and in that case make the whole video look outdated. The advantage of the white board and green screen approaches is the personal touch which is created when the teacher appears on screen him- or herself and directly speaks to the students.[14] As with pre-class introductions only based on audio, the screen capture approach is lacking in developing this personal bonding with the teacher prior to the face-to-face sessions in class. However, it is very important for the teacher to feel comfortable with appearing in front of the camera and to stay authentic. I have seen many colleagues who do not feel comfortable in front of a camera speaking to invisible students. This is something you can see from the first moment of watching their videos that they feel uncomfortable and lose their way in front of the camera. In this case it is strongly advised to use the screen capture approach or to simply use audio only. It will suit the personality of the teacher much better. But this not only counts for the pre-class introductory options where the teacher is not visible. Also,

---

[8] Davis / Neary / Vaughn, 'Teaching Advanced Legal Research in a Flipped Classroom' (n 6) 14; J Ireland, 'Blended Learning in Intellectual Property: The Best of Both Worlds' (2008) 18 Legal Education Review, 150; M Le Brun / R Johnstone, *The Quiet Revolution: Improving Student Learning in Law* (Law Book Company 1994), 260; P McKellar / P Maharg, 'Virtual learning environments: The alternative to the box under the bed' (2005) 39 The Law Teacher, 48; M Şahin / C Fell Kurban, *The New University Model* (FL Global Publishing 2019) 157; Upchurch, 'Optimizing the Law School Classroom through the 'Flipped' Classroom Model' (n 6) 5.

[9] Upchurch, 'Optimizing the Law School Classroom through the 'Flipped' Classroom Model' (n 6) 3.

[10] For more details on *Camtasia* see: https://www.techsmith.com/video-editor.html.

[11] For more details on *Snagit* see: https://www.techsmith.com/screen-capture.html.

[12] Upchurch, 'Optimizing the Law School Classroom through the 'Flipped' Classroom Model' (n 6) 3.

[13] Wolff / Chan, *Flipped Classroom for Legal Education* (n 7) 50.

[14] Wolff / Chan, *Flipped Classroom for Legal Education* (n 7) 50 (n 382).

when the teacher decides to appear in front of the camera, it is very important that he or she stays authentic. The students know their teachers and see them regularly in class. Therefore, they expect their teacher to be the same person in class and in front of the camera. If the teacher tries to be someone else in front of the camera it will irritate the students and diminish the credibility of the teacher's message on video, unless he or she plays a certain role for didactical reasons.

According to my own experience of many years teaching following the *Flipped Classroom* approach, the most effective way to deliver pre-class content in the form of videos aiming at attracting the students and keeping their attention is the advanced green screen approach. Therefore, I also used this approach for the first part of my distance teaching concept: I record myself in front of a green screen, talk to the students while looking in the camera and addressing them directly. This puts me in the centre of their attention and makes the students feel as if I am communicating the message only to them. Seeing me as their teacher in person on video also creates a familiar and comfortable classroom atmosphere for the students as they know me as their teacher and instructor of the course. Using a green screen as background of my video shooting also enables me to place myself in the scene of the topic when I exchange the green background with a photo or picture. In other words: I can already visually connect myself and my message with the topic I explain and thereby create a setting which I would even not be able to create inside the classroom. For example, when I explain some procedural rules of parliament proceedings, I place myself in the plenum of the parliament, where I explain something about the composition or competences of the EU Commission, I place myself right in front of the Commission building in Brussels. I also make use of written text in my videos, for example by slides or pop-ups including some keywords or short headlines corresponding with the things I am explaining. This visually underlines the core content of my introduction and helps the students to keep these points in mind. And, if appropriate, I sometimes also include some interactive elements in my videos, for example by interspersing some questions inside the video or by using tools like *EDpuzzle*[15] or *PlayPosit*[16] for adding images, text, quiz questions and discussions to existing videos. These little technical effects have a big impact on how effectively the students receive and remember my explanations.



To be able to record these videos, I made use of the technical equipment I bought some years ago when I was regularly using the *Flipped Classroom* method at my former university in Istanbul and produced most of the pre-class videos at home on my own. I set up my own little studio in a corner of my living room with a camera, tripod, green screen and lighting. There, I record the videos for my distance teaching lessons. After recording, I transfer the video from the video camera to my computer. For the editing I use some professional editing

[15] For more details about *EDpuzzle* see: https://edpuzzle.com/.
[16] For more details about *PlayPosit* see: https://go.playposit.com/.

software called *Avid Media Composer*. This software is a powerful SD and HD video editor for the PC that offers integrated DVD authoring, surround sound audio processing, and thousands of amazing real-time effects.[17] It enables me to edit the recorded videos in a way that they look professional and include all features and effects which I have in mind to make the content more interesting and to keep the students' attention.

After having finished the video editing, I convert the fully edited video to the MP4 format. MP4 files are MPEG-4 video files, which stands for a compressed file format that can contain not only video but also audio and subtitles. The file compression can be chosen according to the desired resolution of the video. Average quality HD resolution is sufficient for social media, higher quality HD resolution should be chosen for tablets or computer monitors. In general, MP4 format is commonly used for videos uploaded on the internet.

With the recording and editing of the introductory video, the first part of my distance teaching approach is done: the provision of the lesson's main content including learning objectives and assignments for additional material and further reading.

W = *WhatsApp* group discussion.

The introductory videos being my key instrument for addressing the students at the beginning of each lesson, must be made available to the students. Therefore, I had to make up my mind how to distribute the videos. My aim was to find an easily usable and accessible platform which is already part of each student's normal life. The university's learning platform would have been an option. But the *ILIAS* learning platform is not easily accessible on every device and not very convenient to handle. Therefore, social media sources turned out to be the better option for me. They only had to provide the possibility of being suitable for sending and receiving messages of any kind (text, audio and video) and for creating a closed group chat for each course. As all students at my German university used *WhatsApp* on their smartphones, this messaging service became my first choice.[18] *WhatsApp* is a messaging app that uses the internet to send messages, images, audio or video.[19] So, I created a *WhatsApp* group for each course and asked the course representative to add the whole amount of course participants. As the students already used *WhatsApp* as a communication platform among themselves, it was easy to create these *WhatsApp* groups for each course and add all the participants. I first thought that some students might have some concerns in terms of data protection. However, among the more than 500 students who I taught during the Covid-19 virtual learning period, there was only one student who complained about using *WhatsApp* as a communication tool for the course. She pointed out that by using *WhatsApp* as communication platform for a university lecture, there was no clear separation of business and private sphere anymore. Therefore, I did not make it compulsory for the students to join the *WhatsApp* group of our course. However, at the end all the students did join the group. Even the student who was reluctant at the beginning joined at the end after her classmates argued that there was no significant difference between using *WhatsApp* only among the students in their private group and using it for a course including the teacher. Just to offer an alternative communication channel for students who might not have wanted to join the *WhatsApp* group of the course, I also opened a special folder for each course on the university's *ILIAS* learning platform.

After a *WhatsApp* group was set up for each course, it became the key communication

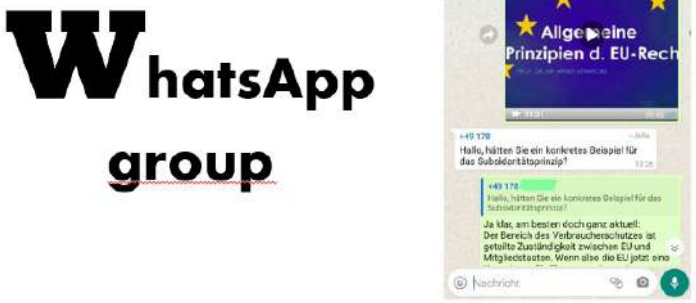
[17] For more details about *Avid Media Composer* see: https://www.avid.com/en/media-composer.

[18] In other countries some students preferably use *Viber* or *Telegram* as their main messaging app. These two messaging apps would have also been technically appropriate for my aims as they include the same features as *WhatsApp*, however, there might be some confidentiality concerns with these messaging apps.

[19] For more details about *WhatsApp* see: https://www.whatsapp.com/features/.

channel between the students and I as well as among the students of each course. At the beginning of each lesson, I posted some introductory remarks in the *WhatsApp* group and then uploaded the introductory video for the lesson. This was the quickest and easiest way to distribute the material to the students. In parallel, I also uploaded the videos on the university's learning platform *ILIAS*. As the university-run learning platform it is the usual place where teachers and students find all necessary information about their courses, including the syllabus, the course content, the dates of the lessons, announcements, assessments and all necessary material for their classes, it is also a suitable place to store the introductory videos for each lesson.

From that moment on, when the introductory video was uploaded on *WhatsApp* and made available for the students on the learning platform, the students became the active part of the distance lesson.



To enable the students to understand and to become familiar with this new way of distance learning, I had to explain my approach and teach the students how to view the pre-class videos effectively. This had to be done right at the beginning of each course, otherwise the whole idea of effectively practising the video-based distance teaching would have failed as most of the students did not have any experience of this approach.[20] The students especially needed to become familiar with using the video as a learning tool. Therefore, they had to experience how to grasp the main content of the video by using pause, go back and replay (parts of) the video, in order to make their notes. To explain my distance teaching approach and to demonstrate the students how to use the introductory videos effectively, I recorded a general introductory video for each course before we started with the actual course content. To create some familiar course atmosphere for them, I placed myself in their actual classroom at university via green screen and illustrated my concept of distance teaching. The after-class evaluation showed me that the students highly appreciated this personalised course-tailored approach.[21]

With the uploaded introductory video to each lesson, including related assignments as well as links to additional material and further reading placed in the course folder on the university's learning platform, the students are equipped with the information they need to work on the lesson topic on their own in the so-called individual space. The uploaded material provides them with an introduction to the lesson, explains the main content and

[20] Şahin / Fell Kurban, *The New University Model* (n 8) 158.

[21] Student comments from the course evaluation of my courses in "German Constitutional Law", "EU Law" and "German Foreign Policy" in June 2020 at the Federal University of Applied Sciences in Brühl / Germany.

gives them short assignments preparing them for and making them curious about the lesson topic.

The preparation for this kind of distance teaching is much more time-consuming than simply giving a lecture, either face-to-face or in a virtual classroom. Firstly, you need to write a screenplay, set up the technical equipment for recording, record yourself, transfer the recorded video to your computer, edit the video and finally upload it for the students. For each video this is a workload of several hours. However, the work for the teacher is not done by having uploaded the introductory video plus some additional material. Mainly during the originally scheduled class time but also beyond, the teacher needs to be available for the students. In my case, it usually takes at least about half an hour before the first students post some questions or comments concerning the introductory video, material and assignments in our *WhatsApp* group. Either I reply in form of a text message or I record a voice message to explain what the students asked me about. As all posts in the *WhatsApp* group are visible for all members of the group, it quite often happens that the students themselves try to give the answer to a question being raised by somebody else or that they start discussing the topic among themselves. This is always good feedback for me, showing me that the students are really engaged with the topic. Some of the raised questions or comments even show how deeply some students are getting into the topic. Another advantage of the *WhatsApp* group is that students do not ask the same questions twice. Everybody is aware of the questions and comments which were posted already. So, there is no redundant waste of time because of the same questions being asked several times by different students. And if so, I just refer to the answers being given above.

As some students – as is the case in the normal classroom – do not feel comfortable asking questions in front of their classmates because they are afraid of asking something stupid, I also offered the students to send me a private message on *WhatsApp* in case they do not feel comfortable posting anything in the *WhatsApp* group. When students do so and when their question including my answer might also be of interest for the rest of the group, I ask the student who contacted me in a private message for the permission to share the posed question including my answer in the *WhatsApp* group of the whole course. Until now, none of the students refused that request. I even had the impression that it made these students more confident when I told them that it was a good question which was worth being shared with the rest of the group.

It is important to mention that teachers should always keep in mind not to overload the students with work while practising this kind of distance teaching. This encompasses both, introductory videos and additional material and assignments: watching an introductory video plus reading some additional material and doing some related assignment is already lots of work for the students.[22] Therefore, the total workload for the students should be kept short and simple, in order to motivate and not frustrate them.

The additional material and/or assignments added to the introductory video, always need to be clearly and understandably connected with the video. This can easily be done by referring to this material or by introducing an assignment already inside the video. Ideally, the legal term, concept, problem, or case being introduced in the introductory video should be reinforced in assigned links or reading. Questions should also be included in the middle and at the end of the video. Questions inside the video are meant to support the process by checking the students' understanding and memory. Questions at the end of the video enable the students to already think about how to use the information being provided for the lesson

[22] P Redmond / C Roper, *Legal Education and Training in Hong Kong Preliminary Review: Summary of Consultation Paper* (2000) 22, 25, 35 <http://www.hkLawsoc.org.hk> accessed 23 June 2020; Wolff / Chan, *Flipped Classroom for Legal Education* (n 7) 59.

topic, for the whole course and for their future legal practice.[23] The idea behind using questions of any of these types is that the students will increase the transfer of the given information into their long-term memory by doing short retrievals during their learning process. This effect is scientifically proven by the learning strategy of retrieval practice.[24]

Z = *Zoom* online consultation hour.

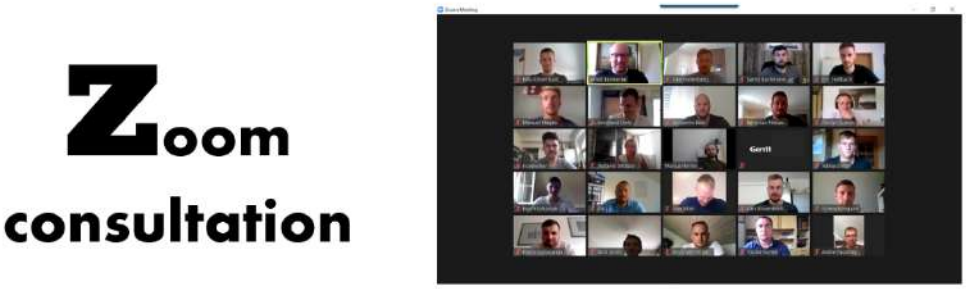
The most important part of a traditional lesson usually takes place inside the classroom when teacher and students meet face-to-face. Although the introductory video plus related additional material and assignments provided understanding and memory of the introduced topic, they cannot fully replace the in-class time. Because the time inside the classroom shows if the students have understood and internalised the topic and if they are able to apply, analyse and evaluate it for their studies. Having provided my students with the necessary material and input for a specific topic of a single lesson, I needed to find a way to check their understanding of the topic. In other words: I was looking for a way to assess if the students actually achieved the learning objectives. Although the communication in the *WhatsApp* group of each course was rather lively, not all students actively participated in the discussions there. As I did not know the students face-to-face from the real classroom, I could not assess if all of them were able to fully follow the course. Therefore, I was thinking about means to hold an additional meeting for the whole course in a virtual classroom. Because I made the best experiences with the *Zoom* for holding a meeting online, this platform was my first choice. *Zoom* unifies video conferencing, simple online meetings, and group messaging into one easy-to-use platform. Apart from easy use and accessibility, its big plus is that it is cloud-based and therefore does not suffer from poor university servers as *BigBlueButton* does, which is incorporated in our university's learning platform *ILIAS*. For holding online meetings with each of my courses in a virtual classroom in addition to the video and *WhatsApp* group, I was considering two options: the first option was to schedule an online meeting for the last 15-20 minutes of each lesson to check if all students successfully understood the core content of the lesson. The second option was to hold a separate online meeting at the end of each week or latest after having finished a set of connecting topics to check if the students achieved the learning objectives of the lessons of the entire week. At the end I opted for the second option. The reason was that, according to my understanding of distance learning, I did not want to force the students to watch the introductory video and to do the additional reading and assignments exactly at the time when our lesson was officially scheduled by the university. For me, distance learning means that each student must have the freedom to wade through each lesson topic anytime and anywhere he or she prefers and, maybe even more important, according to his or her own learning speed. Practising distance learning, each student should also be able to benefit from its positive features. Therefore, it would have been counterproductive to force the students to do their work exactly at the time of the originally scheduled lesson. In case some of them did not finish the lesson in time, an online meeting checking if they understood the lesson content would not have been reasonable. And the reality confirmed this estimation: in many cases, I received questions and comments on the lesson content far beyond much later after the official lesson time. Sometimes, students even wrote me close to midnight because some questions came up while there were working on the topic. So, it was a good choice to choose holding an online meeting on *Zoom*

---

[23] Compare Şahin / Fell Kurban, *The New University Model* (n 8) 160.

[24] PK Agarwal / HLIII. Roediger / MA McDaniel / KB McDermott, *How to Use Retrieval Practice to Improve Learning* (Retrieval Practice 2013) 4 <https://firstliteracy.org/wp-content/uploads/2015/07/RetrievalPracticeGuide-for-FL-Workshop-on-Brain-Based-ESOL-Instruction.pdf> accessed 23 June 2020.

in each course just once a week or at the end of each set of connecting topics, to give the students the opportunity to finish the workload of the whole week in time with their approach to learning.



In our *Zoom* meetings I asked all the students to use their camera so that I could see everybody on my screen and directly address a person when I had doubts about his or her understanding of the course content for the week. The fact that I did not have to present any new topic using screen sharing allowed me to see all students of my course (maximum 30) at once on my computer screen. I started with asking the students if they had any questions concerning the topics of the week. Afterwards I asked them some questions to check if they achieved the learning objectives of that week. These online meetings on *Zoom* formed the last part of my distance teaching approach and completed each week of distance teaching in each of my courses.

4. Advantages of the VWZ distance teaching approach.

Every type of educational strategy or teaching and learning approach has its strong and weak points. The course evaluations of my students were overwhelmingly positive. As most of my teaching colleagues only carried out a one-sided distance teaching approach by either solely doing online classes in a virtual classroom or by just sending the students some reading material, my own VWZ-approach combines various means of distance teaching. In particular, my students highly appreciated the introductory videos for each lesson and the 24/7 availability on *WhatsApp*. They praised that the videos included the most relevant content of each lesson topic providing them with useful guidance through the topic and explanations on how to make best use of the additional material and legal texts. They also emphasized that the videos offered them distance learning at their own speed and time preferences. Beyond that they mentioned that they felt being taken care off even better than in normal classes being held at university, because they felt directly addressed in each video and also had the feeling that they could get in contact with their teacher anytime they wanted.[25] No questions remained unanswered, neither in the *WhatsApp* group nor on the weekly *Zoom* meetings.

[25] Student comments from the course evaluation of my courses in "German Constitutional Law", "EU Law" and "German Foreign Policy" in June 2020 at the Federal University of Applied Sciences in Brühl / Germany.



From the teacher's perspective, the VWZ-approach showed to have the following advantages: A first main advantage of the VWZ-method is that it promotes student-centred learning. The students have more control of the whole learning process. They can access and watch the introductory videos and additional material that is provided online anytime and anywhere and as often as they want or need. This offers the students the possibility to learn at their own pace, according to their own technique and in their preferred learning environment. The lesson content is more and easier accessible than usual.

Closely connected with this advantage is the benefit that students who are not able to attend a certain lesson for some reason such as illness, are easily able to catch up on the missed lesson by accessing the videos and additional material online and work through the lesson content on their own. In case of any questions, they can also easily contact their classmates or the teacher on *WhatsApp* and ask for help or assistance.

Beyond that, the VWZ-approach enhances collaboration between the students and the teacher as the teacher can answer questions and intervene in the group discussions on *WhatsApp* anytime to assist, correct, or clarify during the learning process.

Finally, as a benefit for the teacher, once prepared, the implementation of a VWZ distance teaching lesson takes less time when holding it for a second or third time. The time-consuming preparation of the introductory video and the design of controlling the learning objectives falls away. The teacher can build his or her own database of introductory videos that can be reused. If desired, the teacher can even share these videos with colleagues and edit them based on the feedback received.

Conclusions.

When universities were suddenly closed due to Covid-19 lockdown in Germany and other countries, no university teacher was really prepared for switching from traditional in-class teaching to distance teaching. We all had to improvise. And, depending on our own experience and the assistance our universities provided, most of us had to start from scratch. Having taken this new situation as a challenge, I tried to create my own way of distance teaching. My driving force was to make the best out of the situation and, first and foremost, try to provide the best possible distance teaching for my students. Because they suffered from the changed situation much more than we teachers. Therefore, I did not think about how to get through these difficult times as easily as possible, but to provide the best possible outcome for my students, no matter what efforts it takes. The outcome was an approach combining various available means and tools of teaching on distance: Videos, *WhatsApp* and

Zoom – VWZ. This VWZ-approach, which I invented by myself in times of Covid-19, turned out to be a very promising and effective method of distance teaching and learning. This is the result of my personal evaluation and the evaluation of my students who successfully finished at least one of my courses in which the VWZ-approach was practised. Of course, it did not take me from zero to hero. But it left both students and their teacher without any major complaints about distance learning and teaching in times of Covid-19.

However, it is a very elaborate and time-consuming approach. Therefore, its success mainly depends on the teacher's commitment and openness for innovation and the students' motivation to work on their own conscientiously and continuously at home. This responsibility of the students should be expected at University. Therefore, provided with a suitable learning environment, the VWZ-method provides great opportunities to effectively use means of distance teaching by relocating much of the theoretical background from the traditional lecture to the students' individual space, while accompanying and assisting them by electronic means on distance. And the students are even in better control of the learning process as they can work on the learning matters anytime, anywhere, and according to their own learning pace, while the teacher is constantly available for them to provide guidance, answer questions and give them feedback.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Capitalism of digital surveillance and digital disintermediation in the era of the pandemic

ANTONINA ASTONE
Researcher in Private Law at the University of Messina

Abstract

The article examines the phenomenon called 'digital disintermediation' characterized by a shift of a series of activities from businesses to the population.

The databases, which collect personal information and, more generally, data of both private and public subjects, appear vulnerable to hacker attacks; blockchain technology, which seems to have generated a new climate of trust in the safe use of data, is expression, also of digital disintermediation to which, however, is associated with the risk of an intellectual isolation, known as 'filter bubbles'.

But the Covid-19 has reversed course. Now more than ever, the 'social function' that GDPR 679/2016, in recital 4, assigns to the use of personal data emerges.

The intervention of the public Authorities appears necessary to guarantee a correct exercise in the treatment of the data, in all cases this is urgent or necessary.

Keywords: digital disintermediation; blockchain; privacy.

Summary: Introduction - 1. 'Cold wars' and sophisticated technologies - 2. A new climate of trust with blockchain - 3.Digital disintermediation and the risk of 'filter bubbles'- Conclusions.

Introduction

In the era of the 'fourth industrial revolution', a phenomenon called 'digital disintermediation' has emerged: the distribution of knowledge, in the mass communication sector, has been subtracted from traditional media, such as newspapers and television and news is first conveyed through social networks. In the economic field, this so-called disintermediation, has contributed to the consolidation of platforms such as Bla Bla car, Uber, Booking and various apps, which allow a direct meeting between demand and offer of services. Economic activities are moving from the entrepreneur to the population: the sharing economy, through websites web or mobile app, it gives citizens greater autonomy.

The use of Big Data in this system is also fundamental to ensure the functioning of public services and for systems related to artificial intelligence that are increasingly rapidly expanding. More specifically basic is also the category of personal data, which no longer constitute only an essential component of the right to privacy, but have become well in the economic and legal sense.

The General data protection regulation 679/2016, (hereafter GDPR),

aimed at balancing on the one hand the protection of personal data with the social function which, as specified in recital 4 of the GDPR, personal data can pursue[1] .

[1] *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 11.

The GDPR has set itself the goal of restoring the domain of personal data to people, which, however, is entrusted to other subjects, the data controllers, responsible for compliance with a series of rules and procedures. This subjective split, in concrete terms, both in companies and in public bodies, to which the processing of personal data is granted, implies that the various user ids, passwords, more generally, codes, flow into larger archives, making personal data not very sure.

But blockchain technology seems to have generated a new climate of trust expression, also of digital disintermediation which, however, is associated with the risk of an intellectual isolation known as filter bubbles. Being closed in a 'filtering bubble' means receiving information calibrated to our tastes and preferences; they are the algorithms that basically determine what information we need to receive. This system generates immense power for 'digital oligopolists' such as Facebook, Google: information pluralism and, therefore, the freedom of self-determination is at the highest risk.

In this sense, the Internet was associated with one of the many walls that separate and divide man. But the coronavirus that forced humanity to stop and isolate themselves physically thought of reversing the situation. Like 'a two-faced Janus', the other side of the internet emerges, an instrument of communication, information, socialization and solidarity. The crisis, due to the pandemic, highlighted how personal data cannot be conceived as individual rights, based on the model of property rights and how the world is not yet ready for complete digital disintermediation.

1. 'Cold wars' and sophisticated technologies

The Berlin Wall, whose anniversary was recently celebrated, represented the symbol of the 'Cold war', which has seen the Atlantic bloc, on one side, and the Soviet bloc, on the other, for about fifty years. This is a clash made, essentially, with the use of the technologies of the time. Thirty years later, the fall of this wall did not, however, mark the end of the 'cold war', indeed it is more correct to decline the term in the plural, as many 'cold wars' are fought, once again, through increasingly sophisticated technologies.

In the geopolitics of the fourth industrial revolution, telematic systems, functional to the performance of essential public services, critical infrastructures, on which the daily life of the population depends: energy, transport, financial, judicial and health services, are essentially under attack.

At the basis of their functioning mechanisms is the use of data, which is a connotation of the current era: it is not by chance that it is called a 'dated society'.

The European Union intervened with the General Data Protection Regulation Act (GDPR) 679/2016 dictating a regulation aimed to strengthen the control over their personal data and to ensure its safe circulation.

Starting from the premise that 'only if data circulate freely can Europe make the most of the opportunities offered by digital technologies and progress', EU Regulation 2018/1807[2]was also issued, on the processing of non-personal data, in order to eliminate obstacles to the circulation of non-personal data, which still exist, 'or the proper functioning of the digital single market, strengthen trust in cloud computing and change or put an end to cloud computing contracts in a simpler way'. The databases, which collect personal information and, more generally, data of both private and public subjects, appear vulnerable to hacker attacks: the so-called cyberwar, wars of the third millennium, are digital wars, fought with unconventional weapons.

[2] Regulation (EU) 2018/1807 of the European parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European union OJ 61/2018.

The recall of some episodes may be useful to explain the phenomenon: in 2007, Estonia suffered a cyber attack, probably from Russia, through a Ddos which slowed down some services, blocking computer systems, making public transport means unusable, the banking, postal and judicial services. This resulted in a climate of mistrust and insecurity in citizens, who discovered the vulnerability of digital systems, to which personal data and a series of sensitive information functional to the provision of a series of services are entrusted.

Similar mistrust was fueled in 2013, for Snowden case, concerning the publication, on June 5, 2013, by The Guardian, of the mass surveillance programs, put in place by the National Security Agency, and by the corresponding European agencies for the United States and British governments, which should have remained secret. This fact showed that there were insufficient guarantees of adequate protection of the confidentiality of Europeans' data in America. This resulted in the class action, promoted by M. Schrems, which led to a rethinking of the data transfer system from European to US servers with the issue of a more guaranteed system, the Privacy shield[3].

The Agency for information and external security (Aise) and the Department of information for security (Dis) have opened an investigation, in Italy, on Tik Tok to verify the use that the Chinese government makes of sensitive data of Italian users registered on the platform.

2. A new climate of trust with blockchain

The GDPR has set itself the objective of restoring the domain of personal data to people, through the introduction of a real procedure for the processing of the same, which must be followed by the data controller, imposing the principle of data minimization, limiting the processing of data only to those strictly necessary, regulating for the first time the processing of personal data of minors, and introducing the principles of privacy by design and by default, which are included in the context of accountabilty. A completion a series of very harsh penalties that can go up to 4% of proceeds, in the event of violation of European provisions. The rules, however, requires at least a duality of subjects: the data owner and the data controller. Therefore, it is not always possible to know, with certainty, how the data provided are actually used and processed and, moreover, these centralized databases are often subject to attacks by cyber criminals.

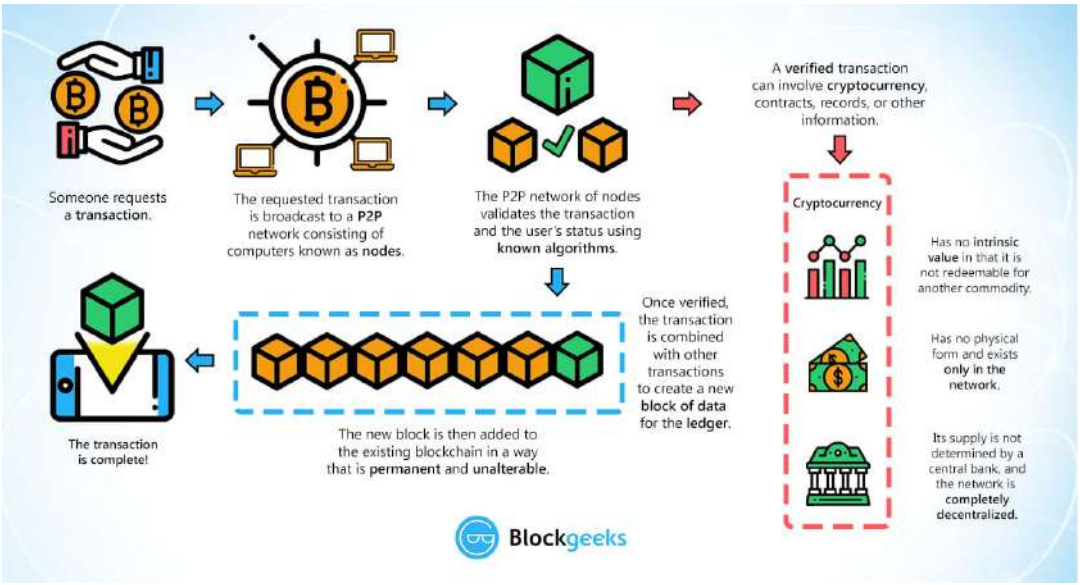
But a new technology seems to have generated a new climate of trust: the reference is to the blockchain which, not surprisingly, arises from a climate of distrust, even if referred to a different area, from that of data. On the occasion of the crisis of subprime mortgages, after, following the bankruptcy of Lehman Brothers to try to save the banking system and, therefore, finance, seriously hanging in the balance on a global level, steps were taken to the detriment of investors of savers: to shake the American economic system and the whole financial world.

In this climate of mistrust towards traditional brokerage systems, a subject who has qualified as Satoshi Nakamoto[4], whose identity is uncertain, could be an individual, a group, a company, created a blockchain. Chain of data blocks is basically a digital register, a database for the management of encrypted transactions, in open source, based on a decentralized

[3] *EU-U.S. and Swiss-U.S. Privacy Shield* Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. On July 12, 2016, the European Commission deemed *the EU-U.S. Privacy Shield Framework* adequate to enable data transfers under EU law.

[4] S.Nakamoto, 'Bitcoin: a peer to peer electronic cash system', in www.bitcoin.com; T.I. Kiviat, 'Beyond Bitcoin: Issues in Regulating Blockchain Transactions'(2015)65 Duke L.J. 569.

peer-to-peer network. Transactions in the register take place via a virtual currency, a cryptocurrency. With the blockchain pemissionless, the subjective split that characterizes traditional data processing methods seems to disappear because the data owner also appears to be the data controller as it determines the purposes (the objectives pursued by the treatment[5]. Obviously an apparent antithesis emerges between the principles on which the scaffolding of the GDPR and the blockchain is supported: if the data in the register are entered in an unchangeable, indelible and irrevocable way, the GDPR allows, instead, to exercise the right to the cancellation of personal data, the possibility to withdraw consent to the processing, as well as the right to request the correction of incorrect data. The information, therefore, in the distributed ledger remains as it was entered the first time and therefore, financial but also health data, military information and other sensitive data are more solid and reliable, and citizens will be able to control, exchange and produce personal data through a computer.



(Graph taken from https://blockgeeks.com/guides/what-is-blockchain-technology)

The disintermediation, compared to the centralized methods of data processing, used up to now, allows not only greater security, but also a convenience in making transactions, since the third-party dialogue, such as credit institutions, reference to the sectors in which the blockchain first developed, such as that of financial services, the cost savings that are produced is evident.

The blockchain also ensures greater transparency on the operations carried out through it, making them more easily traceable and has the additional advantage of allowing, concretely and quickly, to exercise the right to limit the processing of data to those strictly necessary.

Born to satisfy private interests, the blockchain tends to extend also to the advertising sphere, especially by exploiting the permissioned system: in Estonia, since 2007, the Once Only Law has been issued, which governs a system based on identity card, which carries out multifunction: health card, document valid for travel abroad, driving license. In Estonia the Government does not use a Permissionless Ledger but, the so-called Permissioned Ledger

[5]In this sense *Solutions for a responsible use of the blockchain in the context of personal data cnil commission nationale informatique & libertés* of Commission Nationale de l'Informatique et des Libertés 24 september 2018, www.cnil.fr.

which, having governance, can be controlled. Citizens can produce documents, vote from home, managing their personal data independently; however, when new data is added, the approval system is not bound to the majority of participants in the blockchain but to a defined number of trusted nodes. The Permissionless Ledger, on the other hand, was born to be open, it does not have governance, as it was designed not to be controlled. But the need to guarantee the governability of the platform 'clashes with the philosophy itself and the advantages envisaged by the decentralized registers'. Malta, followed by France[6] has issued provisions which take into account blockchain-based technologies. In Italy[7], the legislator has started a process aimed at regulating blockchain technology, favored by EU action[8], whose purpose is to promote and encourage the use of technologies based on distributed registries.

The European Parliament has also asked the Commission to evaluate their potential development scenarios . A single European register, which acts as a 'connector' of the blockchain system at the level of the individual EU States which, in turn, act as individuals blockages in the chain would actually promote true European integration through secure data circulation, including qualifications, diplomas, transactions. This unique system would have positive effects, also in the advertising field, creating an efficient circulation of data, in a safe space, as already happens in technologically advanced realities, where the interest in the blockchain system has always been very high. At present, this solution does not appear viable, also due to the digital diversity that is still being discounted at European level.

3. Digital disintermediation and the risk of 'filter bubbles'

The increasingly frequent use of blockchain technology is attributable to a wider phenomenon that opens up to a new phase: the effects of these technological modalities, in various sectors such as financial, environmental, energy, health, transport, education, will be so disruptive, that once again, a worldwide shared legal response is required, which take into account the breakdown of space barriers, operated by the network. In fact, it is not possible to delegate to self-conduct codes issued by the Over the top, which carry in themselves the risk of a conflict of interest, the discipline of a matter of extreme relevance.

Behind the positive effects of the so-called revolution 4.0, in fact, can conceal negative effects that sociology has identified, mainly, in the risk of loneliness: through a new method of using the psychometry, a science that analyzes someone's personality by quantifying it, the profiling activity has spread, thanks to which the platforms sell advertising spaces to advertisers, through the transfer of targeted personal data, made to measure[9].

The digitalization, to which we are exposed daily, through profiling, means that we become more and more recipients of information calibrated on our digital unconscious. The use of algorithms, to selectively identify the information concerning users, through the creation of a specific profile, ensures that the subject's digital identity is built outside of the same. The growing amount of information collected about each of us and from each of us,

---

[6] In Malta they were enacted *Virtual Financial Assets Act*; *Malta Digital Innovation Authority Act*; *Innovative Technology Arrangements* and *Services Act,* on June 4th 2018. France has given legal recognition to the blockchain, with the decree n. 2018-1226 of 24 December 2018.

[7] Decree Semplifications 14 dicember 2018 n. 135, converted into law 11 febbraio 2019, n.12, entitled *Definition of technologies based on distributed registers*, art. 2.

[8] European Parliament Risolution of 3 october 2018 *Distributed Registry and Blockchain Technologies: creating trust through disintermediation,* www.europarl.europa.eu.

[9] C. Segalin, F. Celli, L. Polonio, M. Kosinski M., D. Stillwell, N. Sebe, M. Cristani, B. Lepri, 'What your Facebook profile picture reveals about your personality', Proceedings of the 2017 ACM on Multimedia Conference, 460; Sandra C. Matz, Michal Kosinski, Nave G., Stillwell D.J., *Psychological targeting as an effective approach to digital mass persuasion* (2017) Proceedings of the National Academy of Sciences (PNAS).

on and off line, both through the internet and in real life, creates what is defined the 'digital unconscious'. According to this view, digital information is unconscious to the extent that we are not fully aware of it. We are far from the meaning of the right to personal identity, developed by legal doctrine and jurisprudence, which presupposes a domination of the person over behavioral heritage. Today there is a tendency to create an 'external identity', in which the construction of the identity is no longer the exclusive patrimony of its owner but built by external subjects in an often partial way, and not corresponding to the true identity of the owner[10].

The digital knowledge that derives from it generates an intellectual isolation known as 'filter bubbles'[11]: staying closed in a 'filtering bubble' means receiving the information that interests us, information that is consistent with our prejudices, which are reinforced by the positive echo who get our ideas. All this system excludes the participation of the subject in the free information market, causing a *humus* conducive to the taking root of fake news and speeches that incite hatred. In a new economy, which modifies human behaviors, because it is able to manipulate their choices, it is the algorithms that essentially establish which information we must receive.

This system generates immense power for 'digital oligopolists' such as Facebook, Google e in the era of 'surveillance capitalism' [12], freedom of self-determination is at a very high risk.

If in the United States the first amendment of the Constitution correlates the pluralism of information underlying the freedom of the press, democracy is evident that the danger connected with a 'filtered life' is that the dialectical one and the comparison between opinions, different knowledge, which it is at the basis of the formation of each person's identity.

Cybersecurity is the right way to defend yourself from cyber warfare but cyber immunity is perhaps more important: it is no coincidence that 'coding' has been introduced in Russia, which teaches how to talk with the computer, a matter that should be made mandatory in the world.

In a new economy that modifies human behavior because 'surveillance capitalism' is able to manipulate its choices, media literacy appears necessary, as is expressly stated in the directive (EU) 2018/1808, on audiovisual media services, recital n.59.

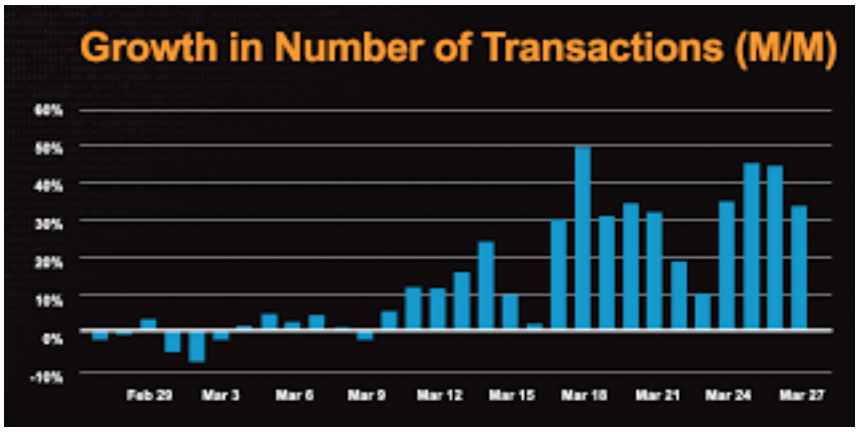
Conclusions: the world is not yet ready for complete digital disintermediation

But the Covid-19 has reversed course, upsetting the frenetic rhythms, to which people had become accustomed, forced humanity to stop and isolate themselves physically. Science, increasingly focused on artificial intelligence developments, was taken by surprise and proved unprepared to cope with coronavirus with appropriate measures. Many politicians thought it was enough to raise yet another barrier to prevent the pandemic.

And it is at this point that like the other side of the network emerges as a formidable tool for communication and socialization.

An invisible virus has highlighted that perhaps the real enemy was not the network which, in such a difficult moment, allows us to meet, launch crowfunding campaigns for the most needy, support healthcare facilities, in the search for drugs and tools necessary for the provision of health services, continue to give lessons to students and rediscover forgotten, but not lost values.

[10] D. De Derckhove, 'Connective psychotechnology' (2014, Milan).
[11] M. Bianca, 'La filter bubble e il problema dell'identità digitale' (2019) MediaLaws. Riv. dir. media, 2.
[12] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (2019, London)



(The graph shows the growth of internet traffic since the start of the pandemic and is taken from https://www.lineaedp.it)

The circulation of data, especially health data, considered 'sensitive data' becomes indispensable both for scientists, to study the progress and remedies for the pandemic and to protect citizens' lives . Now more than ever, the 'social function'[13] that GDPR 679/2016, in recital 4, assigns to the use of personal data emerges.

The surveillance with drones, launched in Italy to check compliance with the Prime Minister's Decree (Prime Minister's Decree) of 22 March 2020, a provision that generally restricts one of the most basic constitutional rights, such as freedom of the person and, specifically, it determines an undoubted invasion of another fundamental right, that of privacy.

The federal government of U.S., through the Centers for Disease Control and Prevention, and state and local governments have started to receive analyses about 'location data from millions of cellphones in a bid to better understand the movements of Americans during the coronavirus pandemic and how they may be affecting the spread of the disease[14].

Democracies, all over the world, appear united, in a tragic and unusual fate, with the Chinese system ([15]), for protection of public health and safety.The European data protection board has issued a *Declaration on the processing of personal data in the context of the COVID-19 epidemic*[16] , where it is emphasized that in these exceptional moments, owners and managers of the treatment must guarantee data which, an emergency situation , represents a legal condition that can legitimize limitations.

In this regard, please refer to: articles 6 and 9 of the GDPR, which allow public health authorities to process also specific categories of data, such as health and biometric data; the e-privacy directive[17] which, pursuant to Article 15, provides for the introduction of legislative measures in situations of emergencies limited to the same.

Therefore geo-localization with mobile devices is allowed provided that the data collected

[13] A. Ricci, 'Sulla "funzione sociale" del diritto alla protezione dei dati personali', On the "social function" of the right to protection of personal data' (2017) Contr. impr., 2, 586.

[14] 'Government Tracking How People Move Around in Coronavirus Pandemic' by *Byron Tau,* The wall street journal, March 28, 2020.

[15] J. Battelle *The search, How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*(London-Boston 2005) 204.

[16] *European data protection board* edpb.europa.eu 20 march 2020.

[17] *EU Directive 58/2002*:Directive 2002/58/CE of the European parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ 2002 L201/45.

is made anonymous, guaranteeing access to judicial protection for citizens. The situation, however exceptional, does not exempt from compliance with the provisions of the Charter of Fundamental Rights of the European Union and of the European Convention for the Protection of Human Rights and Fundamental Freedoms[18]. The compression of the right to privacy of the person is essentially subject to compliance with three fundamental principles provided by the GDPR: proportionality of the treatment, for the purposes that must be achieved; minimization of the data to be used, temporal limitation of this exceptional treatment.

The sacrifice of a fundamental right appears necessary because, on the other side of the coin, there is the protection of the highest value that is at stake: human life.

The Italian privacy Authority[19] calls on all controllers to comply strictly with the instructions provided by the Ministry of Health and the competent institutions to prevent the spread of the Coronavirus without undertaking autonomous initiatives aimed at the collection of data also on the health of users and workers where such initiatives are not regulated by the law or ordered by the competent bodies".

This is the ground on which the immune app is inserted, pursuant to art. 6 of Legislative Decree 29 of 30 April 2020, of which the Privacy Authority, with an opinion of 29 April 2020, recognized compliance with the European Regulation 679/2016 and the guidelines prepared on 21 April 2020 by the European Protection Committee some data.

The application is based on bluetooth technology, allowing you to identify smartphones that have come into contact with that of a positive person. The data must be kept exclusively on the device of the interested subject and can be shared with the owner only when effective contact is found between the non-infected and infected subjects.

The alternative could have been the blockchain that can play a fundamental role in health registers, facilitating access control, transparency, origin and integrity of patient data.

The world is not yet ready for complete digital disintermediation and the emergency legislation caused by the pandemic demonstrate how big data and, in particular, personal data can be a key factor in safeguarding public interests. Therefore personal data, if it is a value that makes up the fundamental right to privacy, certainly cannot be considered in the traditional logic of right *to be alone,* calibrated on the concept of private property, to whose elaboration the jurisprudence of the US Supreme Court has contributed significantly ([20]),

The privacy on the data could infact represent a negative value with respect to the rights in danger, such as the health and safety of the community, and the intervention of the public Authorities appears necessary to guarantee a correct exercise in the treatment of the data, in all cases this is urgent or necessary.

But Google now officially controls the movements of 131 countries affected by coronaviruses, including Italy. It would be "aggregate and anonymous data to show how crowded certain places" developed in "respect for privacy", to evaluate the changes occurred following the pandemic. It's clear that, once again, the Over the top have regained that power over the personal data of citizens that the GDPR wanted to take away from them. If, in fact, it is necessary that the information available for Big tec be used for collective utility purposes,

---

[18] Art. 7 and Art. 8 of *EU Charter of Fundamental Rights*: Charter of Fundamental Human Rights of the European Union, OJ 2010 C83/389; Art.8 of *European Convention on Human Rights*: European Convention for the Protection of Human Rights and Fundamental Freedoms, Sept. 3, 1953, ETS 5, 213 UNTS 221.

[19] Italian Privacy Authority, Coronavirus: No do-it-yourself (DIY) data collection**,** *Rome, 2 march 2020.*

[20] S. Warren, L. Brandeis, (1890) 'The right to privacy', Harvard law review, IV, No.5 193, Supreme Court, *Boyd vs United States,* 116 U.S. 616 (1886); Supreme Court, *Olmstead vs United States*, 277 U.S. 438 (1928); Supreme Court *Goldman* vs *United States*, 316 U.S. 129 (1942); *Silverman vs United States,* 365 U.S. 505 (1961)*; Hoffa vs United States,* 385 U.S. 293 (1966); *Katz v. United States*, 389 U.S. 347 (1967).

on the other hand this should not be resolved on one occasion for further strengthening their power over data.

In any case, users must be adequately informed of this further data flow, which must in any case be addressed exclusively to the public authority, for epidemiological prevention purposes.

Sound as relevant as ever the words of J. Rifkin[21], about the 'new man of the twenty-first century', who is at ease in spending part of his existence in the virtual worlds of cyberspace, manage to change his mask, quickly and quickly, to adapt to any new situation, real or simulated. And so it was: we turned our habits upside down and stopped in the houses to make a social distancing, continuing in cyberspace a life that will return as before but will no longer be the same as before.

[21] J. Rifkin, *The Age of Access: the New Culture of Hypercapitalism* (2021, New York).

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

The (in)adequacy of the law to new technologies: the example of the Google/CNIL and Facebook cases before the Court of Justice of the European Union

ALDO IANNOTTI DELLA VALLE
Ph.D. Candidate in Researcher 'Humanities and Technologies' at University Suor Orsola Benincasa of Naples
Lawyer in Naples

Abstract

The paper starts with the analysis of the two recent decisions of the Court of Justice of the European Union on the Google/CNIL and Facebook cases, also in the light of the GDPR.

The digital revolution is giving one of the greatest transformations to the world since the era of the industrial revolution and is equally aware that we must be ready for the ever-greater penetration of new technologies into our lives. With specific regard to the right to be forgotten, the real problem lies in the fact that personal data become substantially indelible once they have been published online and the only possibility is to think about a possible balance between innovation and the protection of fundamental rights.

For this reason, this paper highlights how both the legislator and the Courts do not pay the due attention to the new technologies behind the law, suggesting a technological approach to law as a way to better protect fundamental rights in the digital age.

Keywords: Right to be forgotten - Data Protection Law - GDPR - Technology - Internet - Search engines

Summary: 1. New technology law and GDPR: the right to be forgotten has been forgotten? – 2. Lack of a technological analysis of the law and weakening of the protection of rights: the Google/CNIL case. – 3. What the Google/CNIL and the Facebook cases have in common: The Court does not care about the technology underlying the application of the law. – 4. The protection of fundamental rights needs a technological approach to law.

1. New technologies law and GDPR: the right to be forgotten has been forgotten?

The Internet revolution has affected every sector of social life and, consequently, has also profoundly changed the face of the legislation, which must inevitably react to these changes to preserve its effectiveness and social utility.

It is, therefore, crucial to reflect on the adequacy of the law with respect to the technology it intends to regulate. In fact, in the 21st century, the development of new technologies is so fast that it requires a constant interaction of legal experts with specialists from other branches of knowledge, who are involved in studying technologies from a technical point of view. Only by being aware of the technical world that is about to regulate, lawmakers and judges will be able to try to keep pace with the development of new technologies and, if possible, to anticipate them. Furthermore, only thorough a knowledge of the technology involved in laws and decisions it is possible to critically analyze[1] them, as we will try to do in this paper.

[1] *See* L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Pol. Dir., 339.

It seems appropriate to start reflections on the topic of the adequacy of the law to new technologies from the analysis of laws and decisions regarding the right to be forgotten, being one of the rights that have become central in the digital age. It changed its skin, becoming even more important, and it never loosed its connotation of inviolable law.[2] The right to be forgotten, traditionally, was linked to the concept of printed paper; the new right to be forgotten, which we may refer as a right to be forgotten 'online', is linked to the world wide web and needs to be properly distinguished from the first even on a systematic level.

The difference between the two conceptions of right to be forgotten emerges, in evidence, thinking about the same structure of the Internet in which the storage of data and information knows no boundaries and knows no obsolescence, especially if indexed in a search engine like Google, making it much more difficult, or in certain cases impossible, to 'be forgotten'.

As for the legislation, it seems necessary to start from the analysis of the aforementioned Article 17 of the GDPR to try to explain, very briefly, why this is disappointing compared to the ambitious objectives that arise.

Two years after the entry into force of the GDPR, applicable in all Member States since 25th May 2018, replacing the Data Protection Directive (Directive 95/46/EC), the new regulation seems to be for many aspects a disappointment, in terms of the adequacy of the law to the demands of European society and ultimately to new technologies.[3] One of these aspects is undoubtedly the discipline of the right to be forgotten which seems to have been forgotten by the same GDPR, Article 17, which claims to regulate it.

After the groundbreaking 2014 decision of the Court of Justice of the European Union in the Google Spain case (C-131/12), it was reasonable to expect an exhaustive discipline of the right to be forgotten by the European legislator: the new discipline should have taken into account the intense debate of the last few years and should have attempted to bring order and clarity.

Therefore, the GDPR would have really constituted the perfect opportunity to finally dictate a uniform discipline on the territory of the European Union also regarding the right to be forgotten, an occasion that unfortunately seems to have been wasted.

In fact, the aforementioned Article 17, paragraph 1, only establish the principle according to which the interested party, under certain conditions, has the right to request the cancellation of personal data concerning him (therefore not de-referencing personal data from the search engine as the Court of Justice claimed in the Google Spain decision). Referring only to the cancellation it is not clear if the GDPR intends to refer this duty to proceed with the cancellation also to the search engines or not.

Definitely, the content of paragraph 1 does not have an original content, if compared with the previous Directive 95/46, Article 12.

Therefore, the right to erasure, as well as the discipline of notification to third parties, was already contained in the previous discipline: the regulation, therefore, only specifies the content of a right already guaranteed on the basis of the previous rules, namely the right to

---

[2] Being forgotten assumes a fundamental importance for the individual who, also if he has committed a fact, has the right not to be remembered for that fact for life, ignoring all his subsequent human and social growth, as well as his eventual reintegration following the expiation of a penalty. In the digital age, being forgotten has become even more difficult, since the web knows no obsolescence. *See* TE Frosini, *Liberté Egalité Internet* (2015) Napoli, 117.

[3] *See* MC Gaeta, 'Hard law and soft law on data protection: what a DPO should know to better perform his or her tasks in compliance with the GDPR' (2019) 1 EJPLT, 61 ff., according to which 'The data protection regulation was adopted in response to the maximum extension of the processing of personal data and to the development of ever more pervasive technologies, strengthening the main EU data protection regime to the point to entail a real reform on data protection'.

erasure, nothing saying about the right to be forgotten, understood, starting from the Google Spain judgment, mainly as the right to de-referencing. Indeed, despite of the heading, the right to be forgotten is neither defined nor disciplined.

However, the same heading of the article, referring to the right to be forgotten, is less ambitious than it would appear, relegating the right to be forgotten in brackets, almost as a subset of the right to erasure. In this way, however, we end up forgetting that the right to be forgotten, if anything, could include the (old) right to erasure, together with the (new) right to de-referencing deriving from the Google Spain judgment. Anyway, the provision seems not to be aware of this, being confused about what erasure is and what oblivion is.

Furthermore, the repeated reference to the element of consent, which certainly constitutes one of the legal bases for the lawful processing of personal data, does not appear at all conclusive[4], especially concerning the search engines and the issue of de-referencing: as a matter of fact, referencing is independent of consent. A regulation based on consent, therefore, will not be able to solve the problems related to the referencing of data which is what really matters when we talk about the right to be forgotten. This aspect, which is now ignored by the GDPR, was correctly understood by the Court of Justice in the Google Spain judgment: it is the presence of those data on a search engine, in fact, to make them truly public on the web, certainly not the presence on an anonymous site lost in the galaxy of the Internet, untraceable for anyone in the absence of an index.

Since it is unlikely that the EU lawmaker would have taken a similar step back from the pronouncements of the Court of Justice, the right to be forgotten, and therefore to de-referencing, would be included in the broader right to erasure. And in fact, consider the right to de-referencing included within the right to erasure is the only way to ensure that the uncertain wording of the GDPR does not weaken the right to be forgotten as emerged in the Google Spain case.

In any case, the answers to these questions will only be confirmed by jurisprudence and, in fact, it is already possible to identify elements by reading the most recent pronouncements of the Court of Justice.

Concluding this brief reconstruction about GDPR, Article 17, the wording of paragraph 2 is appreciated where it expressly mentions the need to take into account the 'available technology', demonstrating to keep in mind the 'technological' approach which should characterize the legislation in these topics. It is very simple, indeed, to impose obligations, if the technology behind it is not taken into account. This type of approach, therefore, should more often be used by the legislator when dealing with topics that, due to their intrinsic characteristics, need a comparison with the technology behind it.

2. Lack of a technological analysis of the law and weakening of the protection of rights: the Google/CNIL case.

[4] About the ineffectiveness of the instrument of consent in order to the processing of personal data see L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale' (n 1), 340 ff.; IA Caggiano, 'Il consenso al trattamento dei dati personali', (2017) 1 DIMT (online), 1 ff.; MC Gaeta, 'Data protection and self-driving cars: the consent to the processing of personal data in compliance with GDPR' (2019) 1 Communications Law, 15 ff.; MC Gaeta, 'La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi' (2018) 1 Dir. Inf., 171 ff.; A Mantelero, 'The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics' (2014) 30 Computer Law & Security Review, 643 ff.; A Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale* (2019) Napoli; J Míšek, 'Consent to personal data processing – The panacea or the dead end?' (2014) 8 Masaryk University Journal of Law and Technology, 69 ff.; DJ Solove, 'Privacy self-management and the Consent Dilemma' (2013) 126 Harv. Law Rev., 1880 ff.

As for jurisprudence, the analysis will start from the recent Google/CNIL judgment[5] of the Court of Justice of the European Union to highlight how this decision neglects to consider the new technologies at the basis of the right to be forgotten. The decision will be then compared with the also recent decision of the Court of Justice in the Facebook case[6], not specifically concerning the right to be forgotten. Indeed, both decisions have in common the lack of adequacy to the technologies they intend to deal with.

Compared to the Google Spain decision, the 2019 Google/CNIL decision certainly represents a step backwards in the protection of the right to be forgotten and a 'good news' for the Mountain View[7] search engine.

The new decision, in fact, territorially delimits the right to be forgotten, limiting the obligation to de-reference to the search engine versions corresponding to all Member States and no longer in all versions of the search engine.

It is appropriate to briefly summarize the terms of the dispute. Already in the aftermath of the Google Spain judgment, Google has considered it a priority to assign a European and non-global value to the right to be forgotten.

Google's approach to the issue of de-referencing was aimed, in essence, to contain 'the damage' to the company resulting from the 2014 decision, recognizing the existence of a de-referencing obligation only with reference to the versions of the search engine whose domain name corresponds to a Member State.

This approach was not shared by the *Commission Nationale de l'Informatique et des Libertés* (CNIL), an independent administrative authority responsible for the protection of personal data in France, which, by the decision of 21st May 2015, has ordered Google to proceed with the cancellation of certain links from the list of results in all versions of its search engine.

In a 2015 document published by Google itself, signed by its Global Privacy Counsel Peter Fleischer and significantly titled 'Implementing a European, not global, right to be forgotten', the search engine had publicly taken a position clearly contrary to the approach made by CNIL. Google even went so far as to say that CNIL's position would make the web the least free place in the world[8].

In support of its thesis, Google stated that the introduction of a generalized de-referencing obligation was disproportionate and unnecessary compared to the purpose, since, according to the data updated to 2015 in the possession of the search engine, about 97% of French users only referred to the local version google.fr, ignoring the others.

---

[5] CJEU, Grand Chamber, 24th September 2019, C-507/17 (Google/CNIL). *See* A Iannotti della Valle, 'Il diritto all'oblio "preso meno sul serio" alla luce della sentenza Google/CNIL della Corte di Giustizia dell'Unione europea' (2020) 2 Rivista AIC, 495 ff.; O Pollicino, 'L"autunno caldo' della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale' (2019) 19 Federalismi.it; G Bevilacqua, 'La dimensione territoriale dell'oblio in uno spazio globale e universale' (2019) 23 Federalismi.it; F Balducci Romano, 'La Corte di Giustizia 'resetta' il diritto all'oblio' (2020) 3 Federalismi.it, 2020, 31 ff.; M Orefice, 'Diritto alla deindicizzazione: dimensione digitale e sovranità territoriale' (2020) 1 Rivista AIC, 2020, 653 ff.

[6] CJEU, Grand Chamber, 3rd October 2019, C-18/18 (Facebook).

[7] P Fleischer, 'Implementing a European, not global, right to be forgotten' [2015], in https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html.

[8] *See* P Fleischer, 'Implementing a European' (no. 7): 'if the CNIL's proposed approach were to be embraced as the standard for Internet regulation, we would find ourselves in a race to the bottom. In the end, the Internet would only be as free as the world's least free place. We believe that no one country should have the authority to control what content someone in a second country can access'. About Google's statement see G Cintra Guimarães, *Global technology and legal theory. Transnational constitutionalism, Google and the European Union* (2019) New York, 155, which observes: 'after all, most companies, Google included, apply worldwide restrictions when they limit access to content that allegedly violates intellectual property rights. If property is enforced globally, so should privacy be'.

Taking note of Google's refusal to comply with the decision taken, the CNIL had therefore imposed a penalty of 100,000.00 euros on Google, with a resolution of 10th March 2016.

Following the CNIL's decision, unfavorable to Google, the search engine manager requested its cancellation by the Council of State of the French Republic (*Conseil d'État*), which had finally referred three related preliminary rulings of interpretation to the Court of Justice of European Union.

With a first preliminary ruling, the *Conseil d'État* asked if the right to de-referencing, as established by Google Spain judgement, should be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester's name is conducted, and even if it is conducted from a place outside the territorial scope of Directive 95/46.

In the event that Question 1 is answered in the negative, the *Conseil d'État* asked if the right to de-referencing should be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester's name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States.

Moreover, in addition to the obligation mentioned in Question 2, the *Conseil d'État* asked if the right to de-referencing should be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the 'geo-blocking' technique, from searches conducted on the basis of the requester's name from an IP address deemed to be located in the State of residence of the person benefiting from the 'right to de-referencing', or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive 95/46, regardless of the domain name used by the internet user searching.

This third question, which undoubtedly would have required a 'technological' analysis by the Court, had been prompted by a proposal by Google itself to the CNIL.

As anticipated, the Court of Justice of the European Union, with the sentence of September 24th, 2019 (case C-507/17), stated that there is no obligation to de-reference in all versions of the search engine[9]. The chosen position, however, was intermediate, since it was considered that this obligation of de-referencing still exists in the domains referable to all Member States (google.fr, google.it, etc.) and not only in the domain referable to the Member State where the request had been made.

The argumentative path followed, and the result achieved by the Court, cannot be free from criticism, since they ignore the advocate general's concerns about technology. [10]

---

[9] The decision is made in relation to a dispute to which the old directive 95/46 was still applicable, repealed with effect from 25th May 2018, but is expressly made also pursuant to regulation 2016/679 (GDPR), whose regulation on the subject of oblivion, as we have seen, cannot however be considered particularly innovative.

[10] The advocate general, in fact, paid wide attention to the resolution of the third preliminary question, relating to the use of the 'geo-blocking' technique to prevent a person from remaining free to search on another version of the search engine. A technique that, it should be remembered, had been proposed by Google itself in the proceedings before the CNIL and which would in any case be circumvented with the use of a proxy server. In any event, despite the attention paid by the advocate general to the technological aspect, the Court does not devote particular space to the resolution of the third question referred or, more generally, to the underlying technological problem. *See* CJEU, 'Opinion of advocate general Maciej Szpunar about case C-507/17', 10th January 2019, in http://curia.europa.eu: '69. On the other hand, if the first question is answered in the negative,

The 2014 decision in the Google Spain case was unfavorable to Google since it guaranteed a right to be forgotten without adequately considering the opposing rights, also entrusting Google with the unwanted role of 'judge' on requests about the right to be forgotten. On the other side, the 2019 decision undoubtedly favors Google's interests, territorially delimiting the protection of the right to be forgotten.

Unfortunately, the decision exposes itself to even greater criticisms than the previous one, not considering that technological developments easily allow to circumvent the scope of the pronunciation and not to take the right to be forgotten 'seriously'.

It is crucial, however, that decisions affecting the digital economy take into account existing technological tools and their adequacy to guarantee the effectiveness of the decision.

Indeed, the Court shows awareness that the de-referencing carried out on all the versions of a search engine constitutes the most suitable way to protect the right to be forgotten. This is because the Internet is 'a global network without borders and search engines render the information and links contained in a list of results displayed following a search conducted on the basis of an individual's name ubiquitous' and that 'in a globalized world, internet users' access — including those outside the Union — to the referencing of a link referring to information regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself'.

The Court, therefore, shows that it is aware of how large the Internet phenomenon is and that deindexing in one version of the search engine cannot, in fact, offer full protection.

In this sense, the decision seems to act almost as an implicit invitation to the EU lawmaker to better regulate the right to be forgotten, since it is stated that 'currently, there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject, as the case may be, following an injunction from a supervisory or judicial authority of a Member State, to carry out such a de-referencing on all the versions of its search engine'.

Although there is awareness of the weakening that the decision will impose on the protection of the right to be forgotten, on the basis of other arguments, the Court states that the operator of a search engine cannot be required to proceed with a de-referencing in all versions of its engine.

The arguments behind the decision essentially relate to the fact that many States outside the Union do not recognize the right to de-referencing or otherwise adopt a different approach for this right: the reference, not too veiled, is to the United States, where the Google Spain judgment received a not too enthusiastic reception.[11] The Court therefore

---

as I propose it should be, such a link is no longer inevitable. As the referring court itself observes, it remains open to a person to search on any domain name of the search engine. For example, the extension google.fr is not limited to searches carried out from France. 70. That possibility may nonetheless be limited by what is known as 'geo-blocking' technology. 71. Geo-blocking is a technique that limits access to internet content depending on the geographic location of the user. In a system of geo-blocking, the user's location is determined with the help of geolocation techniques, such as verification of the user's IP address. Geo-blocking, which is a form of censorship, is deemed to be unjustified in the law of the EU internal market, where it is the subject, in particular, of a regulation designed to prevent professionals carrying out their activities in one Member State from blocking or limiting access by customers from the other Member States wishing to carry out cross-border transactions on their online interfaces. 72. Once geo-blocking is accepted, the domain name of the operator of the search engine used is immaterial. I, therefore, propose to address the third question before the second question'.

[11] For this reason, the Google Spain ruling received a very negative reception in the nation of Google, the United States of America, even on a media level. *See* J Zittrain, 'Don't force Google to "forget"', (2014) The New York Times, 14th May 2014, also online at www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html, according to which: 'This is a form of censorship, one that would most likely be unconstitutional if attempted in the United States'. *See* also G Cintra Guimarães, *Global technology* (n 8), 170, which observes: 'the

affirms that the right to data protection must be considered in the light of its social function and balanced with other fundamental rights. At this purpose, the Court especially emphasizes that 'the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world', also considering that the GDPR, Article 17, has never intended to make any balances regarding the scope of de-referencing outside the Union (not regulating the de-referencing at all).

In fact, through a literal interpretation of both letter b) of the Article 12, and letter a) of the Article 14, paragraph 1, of the previous Directive 95/46, and of Article 17 of the GDPR, the Court clarifies how the EU lawmaker did not intend at all to extend the right to erasure (and therefore the right to be forgotten) outside the borders of the Member States.

In the Court's opinion, currently, the absence of an obligation for the operator of a search engine that accepts a request for de-referencing to carry out such de-referencing on all versions of its engine.

The obligation, however, is to be considered to exist on the domains referable to all Member States, since the European legislator clearly intended to extend, in a uniform way, the discipline regarding the protection of personal data with the choice of the regulatory instrument of the regulation and therefore of a source directly applicable in the Member States: it is precisely the GDPR, therefore, that allows the Court to affirm that de-referencing is to be carried out for all Member States.

However, if some of the Court's considerations appear to be acceptable, making a balance with other fundamental rights, the decision can be criticized in other aspects.

In fact, just like the Google Spain decision, the Google/CNIL decision does not adequately take into account the technological profile and it cannot be considered sufficient, in this regard, to leave Google entirely the burdensome task of taking 'sufficiently effective measures',[12] being totally disinterested in the technical feasibility of protecting the right to be forgotten thus configured and not taking into consideration the easy circumvention that could derive from it.

The Court's idiosyncrasy for the more technical aspects can be seen, first of all, from the substantial failure to answer the third question, not bothering the Court to clarify whether or not the so-called 'geo-block' technique should be used and if this is sufficient to guarantee protection, limiting itself only to imposing on Google the adoption of 'effective' measures.

What matters most, however, even regardless of the application of the aforementioned 'geo-block' technique, is that the territorial delimitation of the de-referencing obligation creates a huge vulnerability in the protection of the right to be forgotten because of a lack of technological analysis of the decision to be made by the Court.

Now, it is true that typing google.com.br or google.co.jp will not be enough to display the results that would appear from Brazil or Japan, thus circumventing the limits imposed by territoriality. However, even if it is not enough to directly enter the URL of a different version of Google, with the use of a proxy server[13] it is still very easy to view a site from Italy as if

---

right to be forgotten […] is a European invention. It does not necessarily match international human rights standards, not to mention the multiple national constitutional standards of different nation states outside Europe'.

[12] Indeed, the Court states that 'it is for the search engine operator to take, if necessary, sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights. Those measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name'.

[13] For the definition of proxy *see* A Luotenen, K Altis, 'World-Wide Web Proxies', in http://courses.cs.vt.edu/~cs4244/spring.09/documents/Proxies.pdf, 1, according to which: 'The primary use

we were in Brazil or Japan, hypotheses that it has been possible to verify personally managing in a few minutes to view Google 'from abroad' while remaining in Italy.

This means that it will always be possible, for those who are really interested in carrying out a 360-degree search on a person, to also trace the results for which the right to be forgotten has been recognized, thus making the (geographically delimited) implementation of that right vain.

The protection would remain effective, therefore, only in front of the average user and not so interested at all in the search for information, which will make only a quick search on his local version of the search engine, without further deepening. On the other hand, the right to be forgotten would be ineffective for all those really interested in finding out who they are dealing with.

The question at this point is: has the Court of Justice actually intended to restrict the scope of the right to be forgotten? Or is the decision only the result of technological inaccuracy?

The Court, on the one hand, showed that she is aware the extent of the Internet phenomenon; on the other hand, however, the worst risk seems to be considered that a person, who is physically located outside the European Union, may view information relating to a person whose center of interest is located within the Union.

These considerations suggest that the Court ignores the real risk inherent in the decision: in fact, as already said, a person, physically located in a Member State of the Union, may display every information for which oblivion has been recognized, through the use of a proxy server, a methodology within everyone's reach with a simple Google search.

3. What the Google/CNIL and the Facebook cases have in common: The Court does not care about the technology underlying the application of the law.

The Google/CNIL decision may be compared with another very recent decision by the Court of Justice of the European Union concerning Facebook (case C-18/18), dated 3rd October 2019, oriented towards completely opposite criteria but that with the pronunciation analyzed above has in common the lack of attention to the technology underlying the application of the judgment.

The present case concerned the sharing, by a Facebook user, on his social network page and without limitation of visibility, of a news published by an online information site. The 'post' included the photo of a member of the Chamber of representatives of the Austrian Parliament and an own comment with contents considered defamatory by Austrian Courts at first and second degree.

Finally, the Austrian Supreme Court decided to raise three questions for a preliminary ruling to the Court of Justice of the European Union, essentially asking if there's a duty on a hosting provider such as Facebook to remove the content of information which is identical to the content of information previously declared to be illegal, or to block access to that information, irrespective of who requested the storage of that information; to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be illegal, or to block access to that information, and to extend the effects of that injunction worldwide.

The Facebook judgement confirms the substantial indifference of the Court of Justice to technological issues, already seen in the Google/CNIL decision, but in a different way. With the decision in C-18/18, in fact, the Court imposes over Facebook an obligation to remove

---

of proxies is to allow access to the Web from within a firewall […]. A proxy is a special HTTP [HTTP] server that typically runs on a firewall machine. The proxy waits for a request from inside the firewall, for- wards the request to the remote server outside the firewall, reads the response and then sends it back to the client'.

contents identical and/or equivalent to those declared illegal, worldwide and regardless of the technical feasibility of what is imposed.

The removal, in this case, would take place all over the world and not only in the Member States, differentiating in this way from the approach followed for the Google/CNIL decision.

In fact, despite the assonances of the issue treated with the right to be forgotten, the 'method' used by the Court to reach the decision appears to be based on different parameters compared to the Google/CNIL judgment, perhaps not adequately justified by the 'silences' of the GDPR about the right to be forgotten and the not too 'richer' wording of Directive 2000/31/EC, applicable to the present case.[14]

It is indeed likely that the Court of Justice wanted to react to the establishment of Facebook's Oversight Board,[15] an own 'Court' on whose effective independence it is legitimate to doubt. The Court is supposed to review content and issue reasoned and binding decisions regarding the contents published on the social network, strengthening a model of private jurisdiction to the detriment of public jurisdiction. Without going further on this aspect, which has already been the topic of specific studies,[16] it seems appropriate to make some observations, in relation to the Facebook case, from the technological point of view. In fact, in the Facebook case, the Court does not care about the technological limitations that would prevent the enforcement of European Union law outside the borders of the European Union, effectively obliging Facebook to implement the codification of very complicated algorithms to ensure implementation in all the world of this principle of law. These algorithms are made even more complicated by the need to find messages with 'the content of which remains essentially unchanged': in fact, how could the algorithm identify those posts that the Court defines as those 'whose content remains, in essence, unchanged' and in 'the content of which, whilst essentially conveying the same message, is worded slightly differently'? Although the Court recognizes that, based on Article 15, Directive 2000/31/EC,[17] there cannot realistically be a monitoring obligation on Facebook,[18] actually it is not clear which algorithm can guarantee an automatic evaluation that has an acceptable margin of error and that does not end up overwhelming activities that constitute a free expression of thought, such as satire.

Ultimately, the Court requires Facebook to use undoubtedly complex technologies whose existence it essentially ignores (nor it seems to worry about them). In this way, it exposes Facebook to the risk of an inadequacy of the existing technology for the law. Therefore, a probable technological inadequacy which however conceals a much safer inadequacy of law compared to the world of new technologies.

In conclusion, undoubtedly the matter dealt with in the Facebook judgment is partially different from that of the Google/CNIL judgment, just as the regulatory framework is

---

[14] *See* Art. 18, para. 1, Dir. 2000/31/EC: 'Member States shall ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved'.

[15] *See* O Pollicino, 'L''autunno caldo", 10 ff.

[16] *See* A Iannotti della Valle, 'A Facebook Court is born: towards the 'jurisdiction' of the future? (2020) 1 EJPLT, 98 ff.

[17] Art. 15, para. 1, Dir. 2000/31/EC: 'Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity'.

[18] In fact, the Court states: 'Differences in the wording of that equivalent content, compared with the content, which was declared to be illegal, must not, in any event, be such as to require the hosting provider concerned to carry out an independent assessment of that content'.

different, but this does not justify such a diversity of approach compared to the Google/CNIL judgment.

The only common aspect, which really links the two pronouncements made after a few days, is the substantial absence of attention to the technology 'behind' the law, beyond the style formulas used here and there.

As a matter of fact, the absence of real attention to the technology underlying the legal statements seems to be the leitmotif of all the pronouncements analyzed, from Google Spain to the most recent Google/CNIL and Facebook pronunciations.

4. The protection of fundamental rights needs a technological approach to law.

As has been shown, what the two relevant pronouncements analyzed above have in common is the lack of real attention to the technology underlying the application of the law.

The European Union is well aware that the digital revolution is giving one of the greatest transformations to the world since the era of the industrial revolution and is equally aware that we must be ready for the ever greater penetration of new technologies into our lives:[19] this, obviously, with the instruments available to the Union itself, and therefore with the law. On the one hand, the reference is to soft law which, in the matter of new technologies, often precedes hard law and tends to occupy its spaces in an almost uncontrollable way;[20] on the other hand, however, there is the awareness that the more serious problems posed by new technologies will require the intervention of hard law.

With specific regard to the right to be forgotten, the real problem lies in the fact that

---

[19] *See* European Commission, 'Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for All', COM (2017) 228, in https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM:2017:228:FIN, where there is a strong awareness of the need for legal intervention in the digital world: 'Successive waves of technological change have transformed human societies and economies, with long-term benefits for both economic growth and quality of life. The current digital revolution has the power to do so again. […] The completion of the EU Single Digital Market also needs a clear and stable legal environment to stimulate innovation, tackle market fragmentation and allow all players to tap into the new market dynamics under fair and balanced conditions. This will provide the bedrock of trust that is essential for business and consumer confidence. […] It is critical for all parties to ensure that the measures are adopted, fully implemented and effectively enforced in a timeframe that is coherent with the fast development of a digital economy. The Commission will bring to bear the full range of policy instruments and funding opportunities to help make this happen, but the full support of Member States, the European Parliament, the Council and stakeholders is essential; otherwise the Digital Single Market will simply not become a reality'. For some initial attempts to implement the European Commission's proposals, see, for example, the proposal for a regulation concerning respect for privacy and the protection of personal data in electronic communications, intended to replace Directive 2002/58/EC with a regulation directly applicable, on the model of the GDPR. *See* European Commission, 'Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)', 10th January 2017.

[20] As far as the European Union is concerned, the reference is evidently to a soft law which is still of European Union origin, such as the guidelines of the European Data Protection Board (EDPB). Precisely on the subject of the right to be forgotten, a consultation was held until 5 February 2020 as part of the procedure for approving the new guidelines, the draft of which is already available online. *See* EDPB, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR', in https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_it. Still on the subject of the right to be forgotten, while remaining at the soft law level, see also the guidelines WP29, 'Guidelines on the implementation of the judgment of the Court of Justice of the European Union judgment in the case "Google Spain and Inc. v. Agencia española de protección de datos (AEPD) and Mario Costeja González" (C-131/12)', 26th November 2014, in https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=667236. With regard to the soft law relating to the protection of personal data, see the aforementioned paper MC Gaeta, 'Hard law and soft law on data protection' (n 1).

personal data become substantially indelible once they have been published online. For example, consider the hypothesis in which personal data is put on the Internet and, at a later time, the same is deleted in the application of the GDPR, Article 17: this does not exclude that someone has already saved the web page that contained personal data on their device. However, that personal data will never be erased.

This is why the Google Spain decision had identified the true form of protection, in terms of the right to be forgotten online, precisely in de-referencing: this is because, even if a personal data still 'exists' on the web and is in fact indelible, it will no longer exist for almost all the web audience, if not (more) traceable through a search engine.

But the delicacy of the issue of right to be forgotten is even more evident with a technological analysis of law. In fact, a technological reading of the aforementioned decisions highlights a considerable vulnerability in the protection of the right to be forgotten, not adequately taken into consideration by the Court of Justice: as has been shown, indeed, it is still possible to access from Italy or from another part of the world to a different version of the search engine where the news has not been de-referenced through the use of a proxy server, a methodology accessible to all and identifiable with a simple Google search.

Therefore, it is crucial to think about a possible balance between innovation and the protection of fundamental rights. At this purpose, the study carried out so far leads to the identification of a method for the protection of fundamental rights in the digital age, based on a serious technological analysis, which should be carried out both by the legislator and by the jurisprudence: it will be possible to provide the fundamental rights in the digital age of a more effective protection only if the functioning of information and communication technologies is really be taken seriously.

More specifically, a technological analysis of law should be based on a hybridization of knowledge.[21] The continuous technological advances of our days require that lawyers interact more and more with technical specialists who are experts in the new technologies that the law should regulate and are aware of the mechanisms underlying their functioning and development. Therefore, taking into account the concrete functioning of the technologies, also interacting with engineers and mathematicians, is sometimes the only way to really verify whether the law has achieved its purpose.

[21] L Gatt, R Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (forthcoming), marks an evolution of the authors' thesis compared to the already innovative perspective of L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale' (no. 1).

EJPLT

Non-personal data processing – why should we take it personally?

NICOLETA CHERCIU
Research Fellow on the Regulation of Robotics and AI at Sant'Anna School of Advanced Studies of Pisa
Attorney at Law
TEODOR CHIRVASE
LL.M. in Law & Technology at Tilburg University
Legal Counsel

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Abstract

Data processing technologies have become more pervasive than ever in recent years, making EU citizens subject to profiling and automated decisions. This article aims to address the issues related to the widely ranging interpretations of the notion of personal data, and to evaluate the extent to which the existing regulatory framework in the EU provides adequate safeguards to the protection of individuals' rights and freedoms in the context of both personal and non-personal data processing operations, identifying the key gaps in the current legal framework that the European Commission and other relevant bodies will need to address to adequately protect EU consumers.

Keywords: personal data - non-personal data - GDPR - consumer profiling.

Summary: Introduction. – 1. The notion of personal data. Uncertainty and fragmentation. – 2. Profiling based on non-personal data. Transparency and accountability gap. – Conclusions.

Introduction.

'Data is the lifeblood of the economy'[1] and it is a very important asset for the future economic and strategic development of the EU market and economy. However, the use of data, when not properly scrutinized and regulated can also have a negative impact on EU citizens' rights and freedoms, as data is being intensively used for profiling, microtargeting, analyzing and influencing the behavior of individuals. An accurate and concise legal framework governing the collection and use of data is thus essential for a democratic and prosperous society. In the EU, data is divided into three categories, namely personal data, anonymized data, and non-personal data. The latter is governed and subject to Regulation (EU) 2018/1807 on the free flow of non-personal data.[2] The first two are regulated by the General Data Protection Regulation ('GDPR').[3] Two years after its enactment, the GDPR was recently subject to the European Commission's evaluation report ('EC GDPR Report'), which found, among others, that although it may be too early to draw definite conclusions

[1] European Commission, *Communication from the Commission. A European strategy for data. COM(2020) 66 final*, 2020) 2.
[2] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L 119/1.

on its success, the GDPR is an important and adequate regulatory tool for the creation of a level playing field for companies operating in the EU and for the strengthening of individuals' right to personal data protection. However, the EC GDPR Report has also identified inconsistencies in the implementation and application of the GDPR, generated mainly by the Member States' use of facultative specification clauses,[4] which may lead to fragmentation and therefore to discrimination with regards to the degree in which citizens of different EU Member States are able to enjoy their rights and freedoms in the digital single market. This paper aims to complement the EC GDPR Report and contribute to the debate on the efficiency of the extant data processing legal framework on safeguarding EU citizens' rights.

To this end, we will first show that the level playing field and protection of EU citizens fundamental rights are hindered by the uncertainty and fragmentation created by the lack of uniformity with respect to the interpretation of the notion of personal data and by the difficulty to distinguish in practice between the three categories of data (personal, anonymized and non-personal). Second, we will show that, although the strengthening of individuals' right to personal data protection has, to a certain extent, been achieved by the GDPR, the emphasis on the protection of personal data unjustly omits to tackle the risks posed by the processing of non-personal data, which mainly arise from profiling based on said data, which can in turn have an impact on individuals rights to self-determination, equal treatment and privacy. Given the risks posed by the processing of non-personal data, the current legal framework focusing exclusively on the protection of personal data and the 'all or nothing' solution enshrined in the GDPR seem to be no longer able to adequately address the risks arising from non-personal data processing. Finally, we propose some remedies to the current accountability and transparency gap related to non-personal data processing and recommend the implementation of procedural and substantive safeguards at EU level for to the processing of such data.

1. The notion of personal data. Uncertainty and fragmentation.

1.1 The notion of personal data.

Personal data is defined under art. 4(1) GDPR as 'any information relating to an identified or identifiable natural person'. Per the same, 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

As per Recital 26 of the GDPR, *anonymized data* is 'information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable' by taking into account all the means reasonably likely to be used for identification, based on the following exemplificative and objective factors: the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.[5]

Non personal data, and more broadly data, is defined under art. 3 (1) of Regulation (EU)

[4] European Commission, *Communication from the Commission. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation. COM(2020) 264 final*, 2020) 7.

[5] Recital 26 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L 119/1.

2018/1807 on the free-flow of non-personal data,[6] as any data other than personal data as defined by the GDPR.

The GDPR and the safeguards provided therein apply only when *personal data* is processed.[7] Conversely, the GDPR does not apply to the processing of anonymized or non-personal data.[8] However, the line between these three categories of data is blurred, and it is often very difficult in practice to draw a clear-cut distinction between them, because (i) the criteria for classifying a set of data as personal or non-personal (ie. content, purpose or element of processing),[9] may be applied differently or ignored altogether by data protection authorities ('DPAs'); and (ii) it is becoming increasingly easier for non-personal and anonymized data to be rendered into personal data by way of combining and/or de-anonymizing data sets.[10]

With respect to *sub (i)*, above, the GDPR definition of personal data, which in essence is similar to the one provided by Directive 95/46/EC.[11] was interpreted by the Article 29 Working Party ('WP') in its 2007 opinion and guidelines ('Guidelines').[12] The Guidelines are the most referenced document when the notion of personal data is analyzed by scholars, data protection authorities ('DPA'), national courts and the CJEU, even after the enactment of the GDPR.

As per the WP Guidelines, *personal data* is any information and statement about a person, whether it is objectively verifiable or subjective in nature, false or true (e.g. subjective opinions and assessments), deducted or inferred;[13] that either: (a) refers to a particular person or it is about that person (content),[14] (b) is likely to have an impact on a certain person's rights and interests, including a minor one (element),[15] or (c) is used or likely to be used to treat in a certain way or influence the status or behavior of an individual (purpose);[16] and the

---

[6] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59.

[7] See in this respect art. 1(1) Recital 26 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L 119/1 whereby it is stated that the 'regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data'.

[8] As per Recital 26 of the Recital 26 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L 119/1, "the principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes".

[9] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136, 2007) 10.

[10] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (WP 203, 2013) 31.

[11] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281/31. According to art. 2 (a) of Directive 95/46/EC, "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

[12] See Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (2007).

[13] Ibid 6.

[14] Ibid 10.

[15] Ibid 11.

[16] The broad interpretation of the notion of personal data was upheld by CJUE in the Nowak case, where the Court held that data relates to an individual when either an element relating to content, purpose, or a result are

(d) processing of said data results in the identification of a person or in the possibility to identify a person. The WP introduced the three-pronged test (i.e. content, element, and purpose) to be applied by controllers and DPAs for determining whether data is personal or not.

Although useful, the assessment criteria proposed by the WP in the test (ie. content, element or purpose) are in themselves a source of uncertainty as to whether a set of data constitutes personal data or not, since the way in which they are formulated leaves room for subjectivity and because they are not applied consistently throughout Member States.[17]

To exemplify, in a recent analysis of digital billboards used to provide tailored advertisement by using inferences (such as gender, age, mood) drawn from anonymized data gathered by cameras equipped with analysis software, the Dutch DPA considered that, since the purpose of processing is ultimately to influence the shopping behavior of passers-by, the anonymized data should be treated as personal data and that the processing operation falls under art. 22 of the GDPR on automated individual decision-making.[18]

On the contrary, when confronted with the assessment of a similar computer vision solution, used for gathering customers' in-store statistical demographics (age, sex, mood, time spent in front of the shelve, etc.), the Bavarian DPA found the data processed to be non-personal, not by applying the three-pronged test but only by looking at the at the risk of de-anonymization. The DPA's argument relied upon the fact that the processing lasted only for 150 milliseconds, after which the images were discarded, meaning that there was a very low risk for the controller or a third party to be able to cross-reference such images with additional data so as to render a specific person identifiable.[19]

Furthermore, the diverging conclusions of the two DPAs in applying the GDPR go even further, since while the Bavarian DPA considered that a 150 milliseconds processing is secure enough to avoid the risk of de-anonymization, the Dutch DPA stated that regardless of the duration of the processing, 'one of the technological possibilities to make data identifiable is to change software settings, (sometimes also remotely) and thus the risk for identification through additional coupling of data still exists'.[20]

Since the Bavarian DPA found that the risk of de-anonymization is low, it has reached the conclusion that the data in question is non-personal, without ever applying the WP test, which, if applied (as shown in the case of the Dutch DPA) may have led to an entirely

present. The purpose element is present when data is used with the intent of evaluating or influencing the status or behavior of an individual or treating the subject in a certain way. See Judgment of 20 December 2017, Nowak, C-434/16, EU:C:2017:994, paragraphs 34-40.

[17] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 6.

[18] The Dutch DPA stated that the data can be used to make automated decisions to show certain ads to certain groups of people or individual persons and the latter may be a decision which affects parties concerned to a significant extent. See in this respect Dutch Data Protection Authority AP, *Digital billboards standards framework*, (2018) available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_branche_normkader_digitale_billboards.pdf (last accessed 16 th November, 2020).

[19] The computer vision solution was used for gathering customers' in-store statistical demographics collecting data such as age, sex, mood, time spent in front of the shelve, etc. Said solution is a technology that enables real-time analysis of customers' faces with regards to their gender, estimated age (range), and emotional state (eg. happy, sad, surprised, angry). The original pictures are neither stored permanently nor processed in the cloud, rather only a transient copy is kept in the camera system memory. The camera software detects the characteristics (metadata) of the person and generates a hash value of the metadata. This process takes fractions of a second. See in this respect Damian George, Kento Reutimann and Aurelia Tamò-Larrieux, 'GDPR Bypass by Design? Transient Processing of Data Under the GDPR' (2019) 9 International Data Privacy Law 285

[20] See in this respect Dutch Data Protection Authority AP, *Digital billboards standards framework,* available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_branche_normkader_digitale_billboards.pdf (last accessed 16th November, 2020).

opposite conclusion.

With respect to *sub (ii)* above, the risk of de-anonymization has been emphasized many times.[21] This risk emerges in the context of big data analytics and powerful AI algorithms, which are able to process, mix and merge different unstructured sets of raw and anonymized data and create second or third generation of data that reveal intimate insights and predictions about individuals (such as political affiliations, sex orientation and purchasing behaviors). The personal patterns and correlations inferred by the algorithms may even be unknown and unpredictable to both the controllers and the data subjects at the time of collection, since these algorithms are characterized most of the time by opacity and self-learning capabilities ('black-box algorithms'). Thus, anonymized data that is linked with additional anonymized data can become personal data.[22]

The two use-cases above show that when deciding on the applicability of the GDPR based on the notions of personal and/or anonymized data, national DPAs need to determine whether a certain data set presents the risk of de-anonymization based on the state of the art. Although the state of the art is an objective criterion, as seen above, it may still be applied differently. Furthermore, even if two DPAs reach the same result in the sense that a data set must be considered anonymized, the final result of the analysis may still be different depending on whether the DPAs apply the WP test or not.

Ultimately, the notion of personal data is always dependent upon 'all the circumstances of the case' and data can be considered anonymized or not only by reference to state of the art anonymization techniques[23] (which is a poor standard considering that de-anonymization techniques evolve at the same pace with data processing methods). While this approach is meant to render the GDPR as technologically neutral and future-proof as possible, the constantly morphing notions of personal data and non-personal data and their different interpretation and application create a certain level of uncertainty, which in turn, raises important concerns, as shown below.

---

[21] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701, Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* 31. Gloria González Fuster and Amandine Scherrer, *Big Data and smart devices and their impact on privacy*, 2015) 18. European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, 2020) 8.

[22] For example, in 2006 Netflix released "100 million supposedly anonymized movie ratings. Each included a unique subscriber ID, the movie title, year of release and the date on which the subscriber rated the movie. Contestants were asked to develop an algorithm that was 10% better than Netflix' existing in predicting how subscribers rated other movies. Just 16 days later, two University of Texas researchers announced that they had identified some of the Netflix users in the data set". See in this respect Julianne Pepitone, *5 data breaches: From embarrassing to deadly* (CNN 2010) (last accessed 16th November 2020).
Also, as exemplified in John Bohannon, 'Credit card study blows holes in anonymity' (2015) 347 Science 468, a team of engineers analyzed 3 months of credit card transactions, chronicling the spending of 1.1 million people in 10,000 shops in a single country. The data was obtained from a major bank. Although the bank stripped away names, credit card numbers, shop addresses, and even the exact times of the transactions and all that remained were the metadata: amounts spent, shop type—restaurant, gym, or grocery store, for example—and a code representing each person, by simulating a correlation attack on the credit card metadata and by feeding the algorithm with a collection of random observations about each individual in the data, the algorithm generated certain clues. The computer used those clues to identify some of the anonymous spenders. The researchers then fed a different piece of outside information into the algorithm and tried again, and so on until every person was de-anonymized.

[23] See Inge Graef, Raphael Gellert and Martin Husovec, *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation* (TILEC Discussion Paper No 2018-029, 2018) 8. European Commission, *Communication from the Commission. A European strategy for data. COM(2020) 66 final*, 6.

1.2 Uncertainty and fragmentation.

The uncertainty surrounding the limits of the notions of personal data and anonymized data may hinder achieving the very aims of the GDPR, namely those of ensuring economic and social progress and of strengthening the convergence of national economies within the internal market, while preserving the well-being of natural persons.[24]

Firstly, different interpretations of the notion of personal data create market fragmentation.[25] While in certain Member States some technologies will be GDPR compliant and thus ready to market, in others they will not. If data processed by such technologies is to be considered personal, the processing operation must be based on a lawful ground,[26] such as consent, which is most likely impossible to obtain for the processing carried out by certain technologies (eg. solutions gathering in-store customers demographics, like those discussed above). Conversely, an easier implementation of such technologies will be possible in Member States where such data is not considered personal data and consent is not required.

Moreover, said differences may impact the implementation of the principles of privacy by design and privacy by default, forcing manufacturers to comply with different standards across the EU.[27]

Further to the above, this uncertainty leads to companies having the space to circumvent the applicability of the GDPR through fictitious constructs and arbitrary standards as to what turns personal data into anonymized/non-personal data (e.g. by measuring the duration of the processing in milliseconds). The lack of foreseeability may also have a potential chilling effect on the willingness of businesses to use data and invest in new technologies.

Additionally, the very purpose of the Regulation (EU) 2018/1807 to ensure the free flow of data may be adversely impacted, as the latter is directly dependent upon the notion of non-personal data, which, if different across Member States, will hinder the possibility to create a uniform data trade environment in the EU. Uncertainty may also create a barrier for the free movement of services, as different interpretations will determine different prevailing technologies across Member States and will distort competition as manufacturers may be incentivized to choose to offer goods and services in some Member States to the detriment of others.

Lastly and most importantly, the same will create different levels of protection across geographies, which will in turn decrease users' trust to use certain technologies and reduce

---

[24] See Mario Viola de Azevedo Cunha, 'Review of the Data Protection Directive: Is There Need (and Room) For a New Concept of Personal Data?' in Serge Gutwirth and others (eds), *European Data Protection: In Good Health?* (Springer 2012).

[25] As stated by the EC, 'fragmentation between Member States is a major risk for the vision of a common European data space and for the further development of a genuine single market for data'. See European Commission, *Communication from the Commission. A European strategy for data. COM(2020) 66 final*, 6.

[26] See Art. 5 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L 119/1.

[27] As per art. 25 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L 119/1, the controllers must implement privacy by design and by default measures. However, art. 4 (7) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L 119/1, defines controller as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. Thus, only when personal data is processed, these safeguards must be complied with.

their willingness to adopt and purchase new technologies.[28] For instance, although the in-store demographics technology implemented in Germany was found to be privacy compliant by the Bavarian DPA, the company had to stop using the system because in-store customers did not accept it.[29]

2. Profiling based on non-personal data. Transparency and accountability gap.

2.1 Profiling based on non-personal data. Risks.

Besides the negative social and economic impact of this current state of uncertainty surrounding the very applicability of the GDPR, we can also identify a potential regulatory gap in protecting EU citizens against the risks of profiling based on anonymized and non-personal data.

Profiling is can be defined as 'the process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category'.[30] Thus, profiles can be either created for an individual or for a group and can be based on any type of data, be it personal or non-personal.

The risks of profiling to the EU citizens' rights and freedoms are manifold, as acknowledged by the WP in its 2018 Guidelines on automated individual decision-making and profiling, which underlines that profiling can perpetuate existing stereotypes and social segregation, lock a person into a specific category and restrict them to their suggested preferences, and lead to inaccurate predictions, denial of services and goods and unjustified discrimination in some cases.[31] Nevertheless, these risks seem to be acknowledged only for individual profiling based on personal data, although – as we will further show below – the risks of profiling based on non-personal data or anonymized data are as significant.[32]

Thus, in the age of interconnectivity and big data, large unstructured non-personal data sets may be linked together and processed by algorithms in ways that can reveal intimate human traits, and even seemingly trivial data (when processed in the same way) may result in the creation of patterns which can be used to predict behavior and to reveal sensitive attributes such as political affiliation, sex orientation, race and purchase behaviors of

---

[28] Similarly, the EC stated that 'citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules'. See European Commission, *Communication from the Commission. A European strategy for data. COM(2020) 66 final*, 1.

[29] See in this respect von WIRED Staff, *Real beendet die Gesichtserkennung in Supermärkten* (2017) (last accessed 16th November 2020).

[30] Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* (Springer 2008), 34.

[31] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev01, 2017), 6.

[32] Profiling is defined by art. 4 (4) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L 119/1 as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'. As clarified by the WP, 'profiling is composed of three elements: it has to be an automated form of processing; it has to be carried out on personal data; and the objective of the profiling must be to evaluate personal aspects about a natural person'. See ibid, 6-7.

individuals or groups.[33]

These inferences and the knowledge obtained from such data may be clustered, aggregated and associated based on different attributes identified by the algorithm, to create certain groups. These groups, which may refer to different segments of the population, are usually not pre-established by the members of the group (such as in the case of a class of students or members of a political party) but are the creation of the algorithm.[34] In this way, the members of a certain group do not even know that they are being categorized as belonging to that group, or that they have been profiled and that their behavior has been analyzed.[35]

Moreover, these algorithms can create spurious and erred correlations and make inaccurate predictions.[36] For example, groups of persons may be profiled as having a predisposition of engaging in a specific type of dangerous activity based on aggregated and anonymous data from a search engine, even though said searches were the result of mere curiosity or popularity of a given topic at a certain moment in time.

This type of information, inferred from non-personal data, can be used in abusive ways absent any safeguards, and may affect individuals even when they are not identified or identifiable. For example, when harmful profiling targets a group, and not an individual, the risks of behavioral manipulation and social sorting arising from profiling are present for the group as a whole and for all its individual members, without ever the data controller having or wanting to know who are the members of the group.[37]

We will provide a couple of examples on the negative effects of profiling based on non-personal data applied at group-level. First, processing data about the purchasing behaviors of a country's citizens to sell lower quality goods in that territory may lead to unfair and misleading consumer practices against all the members of the group.[38] Secondly, allowing advertisers to exclude, based on ethnicity or gender, certain groups from their offerings on housing, employment, and credit history may lead to the discrimination of the natural persons clustered based on these attributes.[39] Thirdly, profiling groups based on algorithmic inferred preferences (ie. affinity profiling) may lead to their members being presented only with certain information (eg. such as in the case of social media networks news feed personalization), thus impairing their access to information. Finally, profiling can exacerbate the phenomenon of digital market manipulation whereby firms exploit consumers' biases and vulnerabilities and use these profiles to dynamically set prices (sometimes to the

---

[33] See Mireille Hildebrandt, 'Profiling: From data to knowledge' (2006) 30 Datenschutz und Datensicherheit - DuD 548 549: 'the data are recorded as a type of brute facts, decontextualized and – as far as the machine is concerned – without meaning. Most data may be trivial in themselves, acquiring new meaning after having been connected with other trivial data and used for decision making'.

[34] Ibid.

[35] Ibid, 550.

[36] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 6 and 12.

[37] "A firm does not need to know specifically who the consumer is to extract rent by exploiting her biases or creating a persuasion profile, only that the observed behavior is that of the same person buying the good or visiting the website". See Ryan Calo, 'Digital Market Manipulation' (2014) 82 George Washington Law Review , 1030.

[38] A recent investigation showed that popular multinational food and drink companies have 'cheated and misled' shoppers in eastern Europe for years by selling them inferior versions of well-known brands compared to products sold in the West. See Daniel Boffey, *Food brands 'cheat' eastern European shoppers with inferior products* (The Guardian 2017) (last accessed on 16th November, 2020).

[39] Julia Angwin and Terry Parris Jr, *Facebook Lets Advertisers Exclude Users by Race* (2016), Julia Angwin, Ariana Tobin and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race* (2017), Jeremy B. Merrill and Ariana Tobin, *Facebook Moves to Block Ad Transparency Tools — Including Ours* (2019)

consumer's detriment), draft purchase and/or website's terms and conditions, minimize perceptions of danger or risk, or otherwise attempt to extract as much profit as possible from their consumers, all of which may ultimately lead to a decrease in consumers' autonomy and freedom of choice.[40]

2.2 Accountability and transparency gap.

Although group profiling based on non-personal data creates substantial risks, this activity is shielded from any accountability and transparency obligations as it falls outside the scope of the GDPR and it happens in the shadows.[41]

Nevertheless, this paper argues that certain safeguards should be adopted even for the processing of non-personal data and profiling based on such data.

For example, individuals should have a right to be informed about their behavior being analyzed based on automated techniques and about the existence of automated decision-making (similarly to the right to information provided by art. 13 and art. 14 GDPR). When profiles are inaccurately created, individuals should have the right to request the rectification of the profile and of the drawn inferences (similarly to the right to rectification provided by art. 16 GDPR).

Since in practice it may be difficult to enforce such rights at an individual level, as suggested by other scholars, the right holders can be the representatives of a group and not all its individual members.[42]

Also, controllers could be made subject to the obligation of maintaining a record of processing activities under their responsibility and to the obligation of carrying out a data processing impact assessment, which shall at least provide an evaluation on the risks to the rights and freedoms of data subjects.

The above transparency and accountability measures can provide individuals with an understanding of how data is being used for their profiling and of what assumptions or inferences are currently drawn about them.

Conclusions.

Even though the GDPR has for the most part reached its aims to enhance data subjects' control over their personal data, there is still room for improvement in what concerns the protection of EU citizens' rights and freedoms from the negative side effects of certain data processing operations.

The processing of non-personal data should be taken seriously and, sometimes, personally. Non-personal data can still be processed to influence individuals' behavior, in which case, under the current status quo, certain DPAs may consider the data as personal data given the purpose for which it is being used. Others may apply the purpose criterion lightly or omit it altogether, in which case the same processing operation may fall outside the scope of the GDPR. Furthermore, even when we leave aside the discussion of whether data is personal or not, the processing of any data, even when it does not refer to a specific

---

[40] See Calo, 'Digital Market Manipulation', 1001. Similarly, see Natali Helberger, 'Profiling and targeting consumers in the Internet of Things - A new challenge for consumer law' in Reiner Schulze and Dirk Staudenmayer (eds), *Digital Revolution: challenges for contract law in practice* (Hart Publishing 2016).

[41] See Hildebrandt, 'Profiling: From data to knowledge', 550: 'as a consequence of the focus on data instead of knowledge, the debate seems to be directed to anonymisation, or the use of pseudonyms, in order to protect personal data. However, citizens may rather need protection against the application of profiles, or at least access to such profiles and transparency concerning their use'.

[42] Linnet Taylor, Luciano Floridi and Bart van der Sloot, 'Introduction: A New Perspective on Privacy' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy New Challenges of Data Technologies* (Springer 2017).

individual, it can still affect him or her.

This current framework creates for companies and data subjects an environment of uncertainty and of lack of sufficient safeguards. It may be that, the 'all or nothing' extant legal framework under the GDPR and the Regulation (EU) 2018/1807 is insufficient, as it does not cover data processing operations which fall under a grey area, namely processing operations where the data does not refer to a specific individual, nor it is about industrial metrics, but to humans in general. Under the current framework, compromises will always be made with respect to humans' data either by considering it as personal, and thus making it subject to the stringent regulatory framework of the GDPR although this data may not always lead to a person being identifiable, or by considering it non-personal, and thus strip its processing of any safeguards.

For these situations, this paper argues for an intermediate level of accountability and for the creation of a regulatory framework for humans' data and for anonymized data which acknowledges the current risks deriving from the processing of non-personal data.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Robots, unwearable profiling and protection of vulnerable users

PAOLA GRIMALDI
Ph.D. at University Federico II of Naples
Lawyer

Abstract

The massive spread of the Internet, the growing use of social networks and the creation of apps have increased and simplified the activity of unaware profiling of users. The phenomenon becomes much more serious when it affects vulnerable users. The GDPR 679/2016 deals very precisely with the issue of profiling personal data by offering adequate protection in several articles by providing adequate security measures to protect users of new technologies and paying particular attention to vulnerable users.

Keywords: Robot - Unwareble profiling - Privacy - Vulnerable users.

Summary: Introduction. – 1. The unaware profiling – 2. Unaware profiling by smart speakers and protection of vulnerable subjects – 3. GDPR and legal protection of vulnerable subjects in automated profiling – Conclusions.

Introduction.

Technological evolution has come to create machines equipped with cognitive abilities and able to interact with humans and the enviroment, showing an ability to adapt independently to surrounding simuli and to assume consequent behaviors; a faculty therefore, similar to the will expressed through a behavioral response (so-called feedback)[1]. The debate of the intelligence of machines started from that strong position[2] of those who imagened that machines would come to think like humans and to be independent; to then fall back on a light position[3] by virtue of which the machines, while showing to be, to some extent, psychologically similar to humans because they can assume psychological states similar to human ones, will not be able to emulate skills and characteristics such as creativity, imagination, intuition, emotion and, above all, awareness of oneself and one's actions[4].

In other words some specific tasks performed by the mind are not algorithmic in nature and, at least for now, cannot be developed by software.

---

[1] P Moro, 'Libertà del robot? Sull'etica delle macchine intelligenti', in R Brighi, S Zullo (ed.) *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica,* (Aracne, 2015), 525-544.

[2] LA Del Monte, *The Artificial Intelligence Revolution, Will Artificial Intelligence Serve Us Or Replace Us* (Louis A Del Monte, 2014) 87; according to which there is no regulatory limitation on the amount of intelligence that can be inserted in a technological apparatus, by 2040 there will be what the author defines "the incredible overtaking" for which the dominant "living" species will no longer be the human one but that of the machines that will acquire self-awareness and progressively conquer the ability to protect themselves.

[3] Position known as the "weak approach to artificial intelligence": to create a new intelligence which, while being characterized from a cognitive point of view, will nevertheless be different from the human one.

[4] For an overview on the topic: E De Santis, 'Computational intelligence and computational thinking: le macchine intelligenti si stanno avvicinando a noi?' <https://www.academia.edu/16172952/Computational_Intelligence_e_Computational_Thinking_le_macchine_intelligenti_si_stanno_avvicinando_a_noi> accessed 28 september 2015.

The light approach to artificial intelligence, supported by authoritative scholars, therefore, does not deny that machines can perform operations that would require an intellectual commitment to humans, but affirms that the intelligence of machines still has a different nature from that of humans.

This last aspect has been explained with reference to the capacity for self-awareness: the intelligence of machines is expressed in conditions of unconsciousness, in the sense that they act "not thinking of themselves".

And in this regard, it is stated that in order to attribute consciousness (or, at least, intentionality) to machines it is not enough to verify that the behaviours and results achieved by a machine do not differ from human ones, but it is necessary to prove that the machine has account of his behavior and really wanted those results[5]; in other words, that there was some willingness to activate the behavior.

The vision of a light intelligence does not exclude a cognitive and behavioral autonomy of the machines, albeit of a technological nature.

In this respect, autonomy rests on data processing and learning processes; in interacting with the environment, machine learn and emancipate themselves, making decisions and behaviors without the intermediation of a closed procedure.

In the machine learning perspective[6], behaviors are not predetermined by the instructions of a software, but are learned from the processing of the experience according to a criterion for improving performance; which implies how said behaviors, although attributable to a learning model, are to some extent non-deterministic and therefore not predictable in their specific unfolding.

In this regard, one can realistically imagine that a robot can assume an initial behavior defined by a software, but also has the ability to modify it after processing a set of data detected, through its sensors, in the surrounding environment.

In this condition, it appears somewhat complex to know in advance which data will be collected and what the new behavior of the machine will be.

The unpredictability of machine behaviors: whoever produces or programs an intelligent machine is able to predict its behavior once it has started to learn from experience? Are these simply objects or do these intelligent machines have to be given some level of subjectivity? Has technology created a new legal entity? Are those non-human subjects able to manifest their own action?[7]

Starting from these questions, there is now a strong need expressed by many to increasingly develop robot law[8], to regulate the behavior of robots and their coexistence with humans[9].

---

[5] GT Elmi, 'I diritti dell'«intelligenza artificiale» tra soggettività e valore: fantadiritto o ius condendum?', in L Lombardi Vallauri (ed.), *Il meritevole di tutela,* (Giuffrè, 1990), 685-711.

[6] When we talk about *machine learning*, we are talking about a particular branch of computer science involved in the study and development of artificial intelligence and we refer to the different mechanisms that allow an intelligent machine to improve its capacity and performance over time. The machine, therefore, will be able to learn to perform certain tasks by improving, through experience, its skills, responses and functions. At the base of machine learning there are a series of different algorithms which, starting from primitive notions, will be able to make a specific decision rather than another or carry out actions learned over time.

[7] On this point see B Bisol, F Lucivero, 'Diritti umani, valori e nuove tecnologie. Il caso dell'etica della robotica in Europa' (2014) 2 Metodo.ISPP, 235, 252; E. Datteri, 'The epistemic roles of automata from cybernetics to contemporary robotics' (2019) 6 RS 245, 256.

[8] In this sense, see P Stanzione, 'Biodiritto, postumano e diritti fondamentali' [2010] CDC 1,15; and also, L Marini, I Aprea, 'Le guidelines on regulating robotics: una sfida per il diritto dell'Unione' 5 (2015) OIDU 1295, 1302.

[9] For an overview of the point: Pontificia Accademia per la Vita, *Roboetica. Persone, macchine e salute*, Workshop 25-26 February 2019.

As part of the debate on the ethical-legal implications of the behavior of robots, there is, among others, the issue of the processing of personal data that they can carry out within the activities for which they were designed, and their compliance with the framework European legislation; the reference, of course, is to the GDPR 679/2016[10].

In this regard, he points out that the processing of data (personal and otherwise) is an essential function of robots in the light of cognitive characteristics by virtue of which they interact with the environment, learn and exhibit autonomous behaviors. In this respect, it should not be excluded that cognitive robots may collect data regarding the users who use them and then transfer them to other people and/or organizations with which the same robots interact.

1. The unwareble profiling.

In general, profiling means any form of automated processing of personal data consisting in the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements of that natural person.

There are three ways of using profiling: general profiling, decision-making based on profiling, decision-making based solely on automated processing.

The legislator pays particular attention to the fully automated decision-making process which also includes profiling, which is capable of producing legal effects or significantly affecting the personal sphere of the data subject; as specified in the guidelines of the European Guarantors[11], it is, concretely, that process in which human intervention is not present or is not significant for the purposes of the decision.

User profiling specifically means the set of data collection and processing activities relating to users of services (public or private) to divide users into behavior groups.

In the commercial field, user profiling is a so-called profiled marketing tool[12], which makes extensive use of this and other techniques to obtain accurate analysis of potential customers, often operating at the limit of the legally permitted, if not beyond[13].

A similar scenario, indeed, re-proposes a question well known in digital news which, from the most recent cases related to the introduction on the market of the so-called apps, date back to the experience of the nineties of the software called *Real Player*[14].

These applications allow access to information and entertainment content, only to discover that the same have been designed to contain instructions for the transmission to other parts of information on the behavior and preferences of users, on their geographical location, often without them are aware.

The massive diffusion of the Internet and the growing use of social networks have

---

[10] G Crea, 'Macchine intelligenti e protezione dei dati in una prospettiva di ethics by design' <https://www.altalex.com/documents/news/2018/02/20/macchine-intelligenti-e-protezione-dei-dati-in-una-prospettiva-di-ethics-by-design> accessed 20 February 2018.

[11] Guidelines on the automated decision-making process relating to natural persons and on profiling for the purposes of the regulation 2016/679, adopted on 3 October 2017 in ec.europa.eu, page Justice and Consumers.

[12] Profiled marketing is a form of advertising that allows you to send personalized advertising messages according to the interests and preferences of users acquired through profiling tools that allow you to collect information suitable for defining the user's profile or personality or analyze his habits or consumption choices.

[13] R Rapicavoli, *Privacy e diritto nel web. Manuale per operare in rete e fare marketing online senza violare la legge,* (Hoepli, 2017) 132.

[14] Regarding the software most downloaded by all users at the time, security researcher Richard Smith discovered in 1999 that there were serious privacy concerns as RealPlayer assigned a unique ID to each user and then subsequently transmitted a list to RealNetworks of all stored media files.

increased and simplified the activity of user profiling. Concrete cases are represented by the "like"button of Facebook or of the surveys that the social network itself carries out through special app[15]; in this last regard, the sensational case is that of Cambridge Alalytica which collected user data through survey applications on Facebook, organized the data with the so-called profiling activity and sold them to Trump and other interested parties, without his know ledge of Facebook users who the Nametest survey app convinced that the results were used for research purposes and, on the other hand, subsequently found their profiles, with all their data, used to target targeted advetising campaigns.

What is even more serious in the story just described is that Cambridge Analytica has also collected data relating to friends of users who had used the app.

This is all due to the fact that Facebook's policies and default privacy settings allow apps to collect huge amounts of data from profiles. It should be noted, however, that Facebook does not work alone in this collection of personal data, but rather finds itself in good company with other giants of the web, such as Google, Netflix, Amazon, Spotify, Youtube and Apple.

In short, the serious risk of finding oneself really in that era defined as *Surveillance Capitalism*[16] with a power in the hands of a few who possess various personal data analyzed in the light of special algorithms, which allow to profile the users of the service, refining their identities digital.

The effect of this activity as described is that an individual will be associated, in a completely unconscious way and without his consent, targeted predictions that outline a digital identity that may even be completely misleading with respect to reality. Sensitive data of an individual, such as personal, genetic, health, behavioral data, could be subject to digital profiling, caging the identity of the same. It is evident that such solutions circumvent the phase of giving consent by the interested parties and, by exploiting their unawareness, they do not even favor ex post interventions to oppose the treatment.

2. Unaware profiling by smart speakers and protection of vulnerable subjects.

The phenomenon described above becomes even more serious when it affects the so-called subjects. vulnerable. And in this regard, there is a wealth of cases that we now have available worldwide, also through the widespread use of the so-called in homes. digital assistants that certainly make our homes more and more smart home, but with the serious risk of compromising our privacy in the place that should represent for us the safest place away from prying eyes and ears.

Smart speakers equipped with a voice assistant are able to collect much more data than a simple Internet search engine and then make them available to companies that already have a huge amount of information on our behalf; think of Google and Amazon[17].

Just to give a few examples, in the United States an important multinational such as Mattel was forced to withdraw the launch of an innovative product such as Aristotle, the first smart speaker designed for children, due to protests and accusations of risk of invasion of the privacy of the same and of an unaware profiling of minors and their families; in Germany the authorities of the German Federal Agency for telecommunications networks have asked their dealers to withdraw the American Cayla doll from the shelves, considered a potential spying tool because, connected via Bluetooth and connected to the Internet, easily hackable, able to listen, record and respond, violating the local national law on telecommunications as it hid a camera and a microphone capable of sending signals and forwarding data unnoticed,

[15]To name a few, survey apps widely used by social networks are Nametest, Toluna and Polly.
[16]S Zuboff, P Bassetti, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, (Luiss Press, 2019).
[17] https://www.gpdp.it/web/guest/temi/assistenti-digitali.

thus damaging the private sphere of people and specifically children, vulnerable subjects from protect and protect even more.

Another case is that of Amazon's *Alexa*, which is also now a famous and widespread smart home device;

for some time, Amazon has been increasingly looking for methods and strategies to use technology as a resource to improve the lives of the elderly and in particular is developing new skills, skills aimed at facilitating the daily life of this growing demographic group which, often, despite the health problems and advancing age, he insists on wanting to live independently for as long as possible. But even for *Alexa* there is no lack of perplexity regarding the real and effective privacy policy of its users put in place by the manufacturer; all considering the "personal data" cases that occurred in Germany and the United States, which concerned the device in question which, after having listened to and recorded a conversation at home, sent the conversation itself, by mistake in interpreting a word heard to some contacts of its users; all this without the knowledge of the latter. It is clear that in this case it was not a human error, but an error of the artificial intelligence system; which leads us to think that, if on the one hand the advantages of technological evolution cannot be denied, on the other, however, it is necessary to approach it with awareness of the potential, but also of the risks, especially when it is the weakest groups who benefit from it. and defenseless of the digital population (children, elderly, disabled, etc. ..).

It is clear that the technology in question must also comply with the rules and principles provided for by the GDPR 679/2016, but to meet the general need to provide strong and targeted protection to those who use such devices, on the European regulatory side there has been the " issuance of the "Cybersecurity Act"[18], a European Regulation which aims to create a uniform and well-defined framework on the certification of IT security of ICT products and digital services; and this, of course, is also of great importance for the smart speaker sector, as the manufacturers of the same must also comply with these new rules in the near future[19].

3. GDPR and legal protection of vulnerable subjects in automated profiling.

The profiling activity has never been the subject of organic and unitary legislation because the regulatory framework has always been very fragmented. Directive 95/46, for example, deals with profiling only with reference to automated decision-making #. In 2002, as a lex specialis with respect to the aforementioned European source, the so-called E-privacy directive (2002/58 / EC) which introduced more specific rules on online tracking technologies (such as cookies), as well as the user's informed consent for their use for profiling purposes. The Privacy Code (Legislative Decree 196/2003), on the other hand, includes the profiling activity among the so-called treatments at risk to be notified, therefore, to the Privacy Guarantor. Finally, the advent of increasingly complex, innovative

[18]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, the European Union Agency for Cybersecurity, and on the certification of cybersecurity for information and communication technologies, and which repeals regulation (EU) no. 526/2013 («cybersecurity regulation»).

[19]The Regulation in question represents an important step for the European Union because it constitutes a clear strategy of strengthening against cyber attacks and the consequent violation of privacy. Furthermore, the legislator's intention was also to strengthen the role of the European Union Agency for Network and Information Security (ENISA) which, therefore, will no longer act as a simple supervisor and assistant to member states in the development of cybersecurity strategies, but will play a concrete operational role because it is used to prepare new European certification schemes compliant with the Cybersecurity Act. These schemes will subsequently be adopted by the EU Commission and will become executive and available to European companies. Clearly these schemes will replace national regulations; it should be noted, however, that, for products certified at national level, their validity will remain unchanged until their expiry.

technologies capable of unprecedented interconnection between users has been a harbinger of new and more appropriate protection strategies: above all for these reasons, during the design and drafting of the GDPR, the need to innovate the regulation of profiling. And precisely with respect to Artificial Intelligence and its multiple applications, the horizon of the topics of competence of the Privacy Guarantor is now boundless. The GDPR 679/2016 in a very precise way addresses the subject of profiling personal data by offering adequate protection in several articles. As specified above, the method of using profiling can also be completely automated and it is in this case that more critical issues are encountered and that the attention of companies, bodies and organizations should increase because in such cases the data collection mechanism for the automated taking of decisions could be based precisely on profiling. The GDPR deals with automated profiling in art. 22, affirming in particular the right of the interested party not to be subjected to a decision based solely on automated processing that produces legal effects concerning him or that significantly affects his person in a similar way. The European Data Protection Committee intervened on the subject and drafted specific Guidelines which, specifically, outline the activities that the data controller will be required to carry out in the event of automated profiling: he must provide, first of all, clear, complete and exhaustive information so that the interested party provides a consent that explicitly allows to pursue profiling purposes which, it should be remembered, according to art. 4 § 4 of the GDPR is represented by any manifestation of free, specific, informed and unequivocal will of the interested party. The possibility of using previously collected data for other purposes is therefore inhibited, unless there has been consent for the specific profiling purpose. Otherwise, it is up to the owner the obligation to implement adequate security measures to protect the data subject. And in this regard, art. 35 GDPR introduces the interesting and innovative institute of treatment impact assessment (DPIA Data Protection Impact Assessment). It applies when a type of data processing based on new technologies creates a high risk for the rights and freedoms of individuals. In this case, the data controller is required to assess the impact this may have on the protection of personal data. The risk inherent in the processing is to be understood as the negative impact on the freedoms and rights of the data subjects and represents the pivotal tool through which the owner carries out the analysis of the risks deriving from the treatments put in place. The owner, therefore, must develop a preventive assessment, before starting the processing, of the consequences of the data processing on the freedoms and rights of the data subjects. Unlike safety assessments, the impact assessment should be developed only for particular treatments, i.e. when the treatment involves the use of new technologies and can present a high risk for the rights and freedoms of individuals. Article 35 of the GDPR indicates the criteria on the basis of which the cases in which the DPIA is necessary are identified. Furthermore, paragraph 5 of art. 35 grants the supervisory authorities the possibility of drawing up a public list of types of processing for which the DPIA is required. In this perspective, our Privacy Guarantor, together with the high European authorities, has prepared a list that has been the subject of an opinion by the EDBP (European Data Protection Committee). In particular, the Italian Guarantor has identified twelve types of treatments subject to the DPIA obligation, listed in Annex 1 to the Provision of 11 October 2018. And the framework envisaged by this list would seem to go in the direction of an expansion of the scope of the obligation of DPIA. In particular, the hypotheses listed in point 6) include that relating to the non-occasional processing of data relating to vulnerable subjects (minors, disabled, elderly, mentally ill, patients, asylum seekers, etc.).

Conclusions.

From all the above, it is clear that personal data has an absolute value that must be

protected and safeguarded in the face of the rapid and relentless development of new technologies in the face of which man's approach should have a double attitude: of awareness with respect to potential of the technologies themselves and of prevention, with respect to the risks that inevitably derive from using them. Certainly, one cannot think of opposing technological development or of somehow curbing the creativity of information technology and, indeed, new technologies and their evolution must be viewed positively if one thinks, as already examined above, of the potential that they can have in covering roles of assistance and support to categories of vulnerable subjects; however, these potentials must be approached with awareness and intelligence, always remaining on guard against the concrete possibility that all this technology can "attack" the privacy of users. Therefore, an attitude of protection of personal data and the adoption of appropriate precautions is essential, even by the same large manufacturing companies that it is hoped that they will proceed increasingly planning according to the framework of ethics values (ethics by design) of which of course privacy is part of it[20].

And following the references made in several circumstances on this point by the Privacy Guarantor, the response of all the protagonists of this sector should be based on the ethics of responsibility to be implemented precisely in the design phase of the technological measures (software) that are able to minimize at the highest level the risks of harmful behavior of robots for the privacy of all, but in particular of the categories of the most vulnerable subjects in society; all this, spreading more and more the culture of the importance of the immense wealth of personal data available; the risks to which the data are subjected on a daily basis; creating awareness of the existing rules and means for the protection and safeguarding of one's privacy and, consequently, of the possibility of demanding the so-called privacy by design from companies that produce in the Internet of Things sector and therefore not adjusting to the passive use of robots, taking into account that companies themselves are responsible for assessing the privacy impact and subject to severe penalties if this is not done correctly. With specific reference to digital assistants, it is clear that they should be technically developed in compliance with the principles of confidentiality and data protection and, according to the GDPR legislation, ensure transparency and control of user information, allowing for concrete data governance.

Anyone who produces AI devices and places them on the EU market cannot disregard the GDPR, as already specified above is required to provide privacy by design in the design, to clearly define the perimeter of the processing of personal data. The principle of accountability returns, for which it would be essential for companies producing AI tools to provide basic technical product information in a transparent manner, which instead are almost never so easily available; and still companies or even consumers themselves should take action for a privacy impact assessment before purchasing and using such smart devices.

[20]A Nunn, 'Does Privacy By Default Mean Researchers Should Reconsiderer Reaserch Ethic Practice in relation to recording Informed Consent' (2018) 1 EJPLT.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Online market, big data and privacy protection

ANTONELLA CORRENTI
Researcher fellow in Comparative Private Law
Lawyer

Abstract

The digital market and the protection of privacy could not fail to be affected by the effects produced by the indiscriminate use of social networks. The objective value of modern communication tools should not be overstated, the impact should rather be monitored in order not to frustrate its inspirational logic. The coronavirus pandemic has made the need for reflection on the issue even more vivid, being the means of distance communication that have become the exclusive means of social interaction.

Keywords: Social networks - Big data - artificial intelligence - digital market.

Summary: Introduction. – 1. Digital era: origins, evolution and implications. – 2. Big data and antitrust. – 3. Binding practices and leverage theory in the digital age. – Conclusions.

Introduction.

In the era of globalization and digitalization, modern multimedia communication tools capture the attention of consumers and users influencing their choices and habits.

Social networks (facebook, twitter, linkedin, google, whatsapp, instagram) constitute the new vehicle for information and marketing: those who use it, through increasingly advanced tools and at competitive prices, use promotional slogans and socialization as compasses for orientation in the intricate forest of the market.

This new trend is not surprising: every day, wherever we are, we use the internet connection and we are able to compare prices and offers of goods and services, and even to proceed with the related purchases.

Much of the work, study, affective and daily life activities can be carried out electronically through mail, chat, browsing which, thanks to their widespread diffusion, have now replaced traditional conversations.

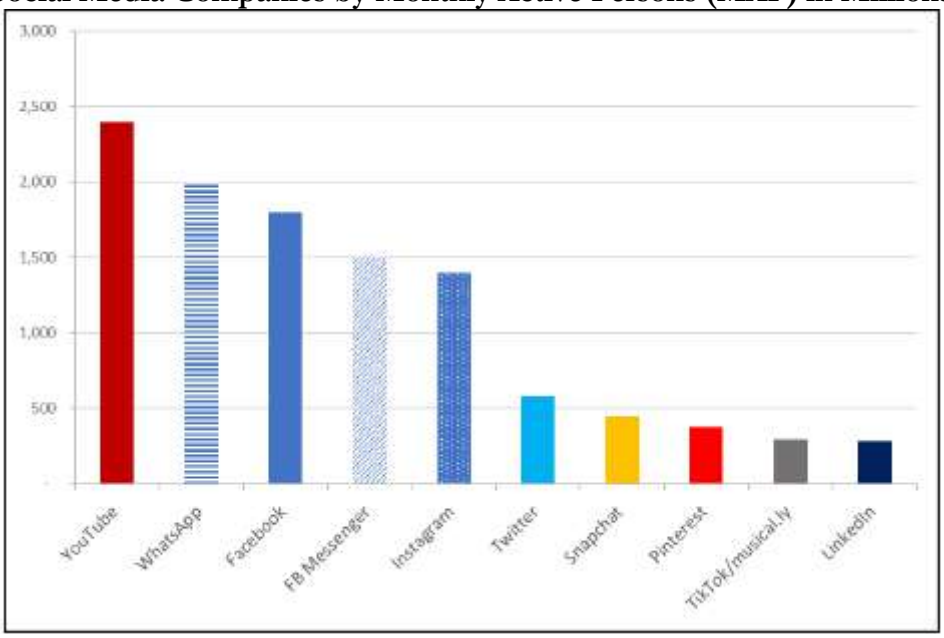
Social networks are generalists and specialists; the former (facebook, twitter, google)[1] are the most common means of interaction and transmission of media and messages; the second category concerns specific types of users or contents: linkedin (professionals), instagram (amateur photos), academia (researchers). To access the related services, you must register: the user declares to accept the general conditions of use, giving consent to the processing of their personal data, which consequently are repeatedly entered into the system and stored[2].

1 Facebook and Twitter represent the two major social networks and, despite the possible simultaneous use, they have different functions. Facebook has a wider operating scope, as it constitutes a more conventional medium and allows you to share more information, photos, updates. Twitter has a more limited application and is an ideal platform for information. Google is the most famous search engine, whose registration dates back to 1997, since then it has acquired such importance as to favor the introduction, in common language, of expressions deriving from the root of the term (for example "googlare" to indicate the web browsing).

2 Registration represents the modern expression of consent to data processing. Most of the personal data collected by social networks pass overseas in order to be processed and / or stored by the parent company: Facebook currently uses four data centers in the United States and one in Sweden; Twitter, on the other hand, takes advantage of already existing data centers by paying space leasing quotas to the managers, who are also all operating within the United States.

The graph below, taken from the report "*Investigation of competition in digital markets*" of the Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary[3], photographs the data relating to users of the most popular sites as of December 2019.

Social Media Companies by Monthly Active Persons (MAP) in Millions



The central role of consent in accessing digital platforms is enhanced by the European legislator in Regulation 2016/679 (GDPR), relating to the protection of individuals with regard to the processing of personal data, as well as the free circulation of digital data.

The Regulation replaced Directive no. 46 of 1995[4], but is the result of a broader regulatory process, started on January 28, 1981 with the Strasbourg Convention on the protection of individuals with regard to the automated processing of personal data. The reference discipline, in order to ensure an equitable distribution of powers and to remedy any information asymmetries that make the position of the interested party more vulnerable, revolves around three main figures: the data controller, the data processor and the interested. The data controller acts as a guarantor and supervisor and must be able to demonstrate that the user has given consent to the processing of their data.

Pursuant to Article 4 (11) of the GDPR, consent is understood as any manifestation of free, specific, informed and unambiguous will by which the interested party legitimizes the processing of their data.

In spite of the automaticity that, from a temporal point of view, characterizes the provision of consent, the latter must constitute a considered choice: art. 7 GDPR, paragraph 3, establishes the right of revocation at any time; paragraph 4 provides for the separation

[3] Investigation of competition in digital markets. Majority staff report and recommendations. Subcommittee on antitrust, commercial and administrative law of the committee on the judiciary, United States, 2020, 92.

[4] The comparison between the wording of art. 1 of Directive 95/46, which provided that States should "*protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*", and the corresponding Article 1, paragraph 2 of the Regulation, which places among its various objectives the need to protect "*the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*" The omitted reference to the concept of confidentiality, in the new formulation, seems to create a clear gap between the need for data protection and respect for privacy.

between contract and consent if the execution of a contract is conditional on the provision of consent to the processing of personal data not necessary for the execution of this contract.

Given the particular context of reference, it is necessary to ask whether the manifestation of consent, sometimes expressed unconsciously, determines a real transfer of ownership over the personal data or a sort of delegation to use the data itself[5].

Depending on the chosen reading, the consequences change, not only for the legal effects produced by one and the other approach, but also for the concrete operation of the privacy regulations and to protect competition.

The thesis of the transmission of a property right on the data would seem to be supported by the provision of art. 20 of GDPR on the right to data portability[6].

The provision performs two functions: to increase the data subject's control over their data and to facilitate their circulation.

A fundamental step, which preceded the GDPR, is represented by the Charter of Fundamental Rights of the Union, whose art. 8 raises the protection of personal data to the rank of subjective right[7].

Faced with situations of undeniable aggression to the private sphere, particularly evident in the virtual world, it is necessary to enhance and enrich the content of privacy to prevent it from becoming "a mere bureaucratic burden, a piece of antiquity destined to succumb to the irresistible charm of sharing "[8].

The unstoppable advance of digital technology leads to a reflection on the ability of current regulatory systems to face the challenges offered by a constantly evolving society and to offer effective and effective protection.

Looking at the European legislation, one gets the impression of an approach detached from the consideration of data as attributes of personality, reasonably dictated by the need to reconcile the rights of the individual with market needs.

By privileging the circulatory moment of information, to the detriment of the content of the data and their representative potential, the prospects for protection and the principles of responsibility and transparency that inspire the Regulation are nullified[9].

It is necessary to combine the ideal and the patrimonial dimension, to strengthen the

---

5 See N Zorzi Galgano, *Persona e mercato dei dati, Riflessioni sul GDPR* (Cedam 2019).

6 The law clarifies that "*The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means*"(art. 20 par. 1 GDRP). See A Maceratini, 'Privacy e informazione nell'era dei Big Data', in *Tigor: rivista di scienze della comunicazione e di argomentazione giuridica* - A. XI (2019) n. 2.

7 The text of the Charter was signed in Nice on 7 December 2000 and re-proclaimed on 12 December 2007, in view of the signing of the Lisbon Treaty, in Strasbourg by the European Parliament, the Council and the Commission (OJEU 14 December 2007, no C. 303). Pursuant to art. 6 paragraph 1, first paragraph, of the Treaty, the Charter of Fundamental Rights of the European Union has, since 2007, the same legal value as the Treaties.

8 See A Thiene, 'Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*'*, in *Nuove leggi civ. comm.*, 2017, 410; M Bocchiola, *Privacy. Filosofia e politica di un concetto inesistente* (Luiss University Press 2014), 149.

9 See G Giampiccolo, 'La tutela giuridica della persona umana e il c.d. diritto alla riservatezza', in *Riv. trim. dir e proc. civ.*, 1958, 458; P Rescigno, 'Personalità (diritti della)*'*, in *Enc. giur. Treccani*, XIII, 1990, 5; P Perlingieri, *La personalità umana nell'ordinamento giuridico* (Jovene 1972), 174; C Castronovo, 'Situazioni soggettive e tutela nella legge sul trattamento dei dati personali', in *Eur. dir. priv.*,1992, 653; F Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679* (Giappichelli 2016); S Sica, V D'Antonio, GM Riccio (a cura di), *La nuova disciplina europea della privacy* (Cedam 2016).

guarantees and offer the consumer a clearer perception of the value of their personal data[10].

Without neglecting the aim of *contributing to the realization of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and convergence of economies in the internal market and to the well-being of individuals* (recital 2 of Regulation), a correct framing of the case under consideration requires the consideration of a concept of privacy in a broad sense, all-encompassing all the evocative aspects of personal identity from the oldest (confidentiality, name, image), to the most recent (oblivion)[11].

In addition to the concern for the damage to the private sphere of users of the variegated world of the internet, there is the risk that interpersonal relationships are entirely replaced by virtual ones and that the desire for connection becomes a real obsession, with inevitable consequences of isolation and pathological addiction. The technological tool makes conversations cold and aseptic by altering the authenticity of the underlying feelings.

The empathic and emotional profile is replaced through the use of algorithms and digital writing; a sort of dehumanization of man arises which must be reconsidered *not as a person alienated from technology but striving to fulfill himself in all his humanity*[12].

The current period is defined as post-modernity, an expression that seems to evoke, not only the distrust and insecurity of today's man, compared to "modern man", but also a regression, from the point qualitatively, interpersonal relationships[13].

The truth lies in the middle: the revolution triggered by the so-called digital feudalism[14] requires an exact identification of the characteristics of the phenomenon to grasp its potential and limits.

An articulated and complex reality emerges which leads to a sort of convergence between the transmission channels and the contents transmitted: a real digital market for which the urgency of a specific regulation is looming.

1. Digital era: origins, evolution and implications.

Technological progress and modern communication tools transform the way of approaching everyday reality, depriving it of the practical, emotional and hedonistic aspects that usually characterize it[15].

To understand the impact and changes that have occurred over time, it is necessary to go back to the origins of the revolution which then favored the development of the internet and the birth of the so-called digitalization. The roots are to be found in the creation of the software industry.

The expression software (soft / light, ware / product) is used in computer science to indicate the set of intangible elements of an electronic data processing system, to distinguish it from the concept of hardware which, on the contrary, refers to the component material of

---

[10] See A Thiene, 'Segretezza e riappropriazione' (n 7) 415. On the contrary, see A Ottolia, 'Privacy e social networks: profili evolutivi della tutela dei dati personali', in *AIDA*, 2011, 363-371, according to which it is necessary to keep separate the asset profiles and personal aspects.

[11] See G Finocchiaro, 'Il diritto all'oblio nel quadro dei diritti della personalità', in *Dir. inf.*, 2014, 591.

[12] See R Pagano, 'Pedagogia e Tecnica. Coincidentia oppositorum', in C Laneve, R Pagano (eds), *La pedagogia nell'era della tecnica. Derive e nuovi orizzonti* (Pensa MultiMedia 2006), 41.

[13] See N Bobbio, *L'età dei diritti* (Einaudi 1990), 263. The author clarifies that we have entered the so-called post-modern era, characterized by the enormous, vertiginous and irreversible progress of the technological and consequently also technocratic transformation of the world.

[14] A Giannaccari, 'La storia dei Big Data, tra riflessioni teoriche e primi casi applicativi', in *Mercato Concorrenza e Regole,* 2, 2017, 313.

[15] On the role of new technologies and the Internet see G Sartor, 'Prefazione', in G Scorza, *Il diritto dei consumatori e della concorrenza in Internet* (Cedam 2006), 1.

the same system[16].

During the IT training era, the software was not marketed separately and 1969 should be expected for the introduction of the related licenses[17]. Since then, licenses have become the main tool for spreading software products in the mass market.

In the 1980s, the software industries began to grant subordinate contractual rights to customers in the form of license agreements; since the 90s new technologies have spread and there has been a proliferation of the internet and digital platforms.

The rise of the digital market opens the frontier to the so-called big data and raises many interpretative questions, dividing those who tend to favor the automatic aggregation and processing of data from those who instead focus on the content of the same[18].

The expression "big data" contains four fundamental characteristics: volume, speed, variety and value. The first two refer respectively to the size of the recorded and stored data and to the speed with which they are processed. The variety concerns the countless sources from which the data can be drawn. The value is the natural result to which the information collection, processing and processing operations lead. Even the behavior of each individual seems to be accelerating as a result of the rhythms imposed by multimedia tools[19].

The issue of data management by digital platforms intersects with that of the economic value of the data itself; despite of the alleged gratuitousness of the service, with internet access, consumers pay IT companies a price represented by the management of the information concerning them.

The concept of privacy therefore takes on a new value, by becoming the same an economic resource sold in exchange for a provision of services[20], which corresponds to an economic return in terms of personal information and sales of advertising space.

The collection and processing of personal data, even sensitive ones, should take place in an adequate and effective way to avoid the risk of aggression to the personal sphere and of incorrect commercial practices.

The Italian privacy legislation emphasizes the need that the processing of data does not affect the rights, freedoms and dignity of the interested party (art.1, Legislative Decree 196/2003) and is carried out only where necessary (art.3) , in a lawful and correct manner (Article 11, letter a).

The data must be stored in a form that allows the identification of the interested party for a period of time not exceeding that required to pursue the purposes for which they were collected (art.11, letter e).

These forecasts often run the risk of being disregarded: and this leads us to evaluate the

16 It is customary to attribute the introduction of the term "software" to John Wilder Tukey, a famous American statistician, who first used it in 1957. Only in 1970 would the relative concept appear in the popular lexicon, but together with that of hardware. It will be necessary to wait some time before a separate consideration.

17 The birth of separate software licenses is linked to the antitrust lawsuit filed by the Department of Justice against IBM, the oldest US company in the IT sector, accused of anti-competitive conduct for the combined marketing of software and hardware.

18 A Giannaccari, 'La storia dei Big Data' (n 13) 309. See also F Di Porto**, '**La rivoluzione Big Data. Un'introduzione', in *Concorrenza e mercato*, 23, 2016, 5-14; AM Gambino, 'Diritti fondamentali e Cybersecurity', in M Bianca, A Gambino, R Messinetti (eds), *Libertà di manifestazione del pensiero e diritti fondamentali* (Giuffrè 2016), 21-30; M Delmastro, A Nicita, *Big data, Come stanno cambiando il nostro mondo* (Il Mulino 2019).

19 G Pitruzzella, 'Big data, competition and privacy: a look from the antitrust perspective', in *Concorrenza e mercato*, 2016, 15-28.

20 Privacy in the digital market includes not only the confidentiality of the individual, but also the protection of personal data concerning him. See S Palanza, 'Internet of things, big data and privacy: the triad of the future', in *IAI, Documents from Istituto Affari Internazionali*, 2016, 9.

possibility of integrating the privacy regulation with the competition regulation in the portion of the market in which the social networks operate.

Among other things, technological development and the increasing level of digitization presuppose the preparation, by companies, of the tools and organizational structures necessary to deal with data and information management which is not always efficient.

The need to reconcile apparently antithetical areas (privacy, competition and consumer protection) arises from the awareness that companies, in exchange for the services offered, acquire market power and are able to predict user behavior or even anticipate its behavior the choices .

The links of reflection widen in an attempt to derive from the specificity of the disciplines involved a univocal key of interpretation and uniform regulation[21].

With a view to promoting a European digital market and protecting the individual in his or her fundamental rights, Regulation 2016/679 (GDPR) moves.

The European institutions on several occasions have highlighted the need to balance the purpose of creating a single digital market and the protection of the processing of personal data and the free movement of the same[22].

In an unexplored context and exposed to various "external aggressions", there is a greater need to intervene in a penetrating and compelling way in the interest of consumers.

Undoubtedly the digital age offers the possibility of new forms of innovation, but the discriminatory footprint it brings requires targeted interventions on several fronts, in order to guarantee the effective safeguarding of users' privacy and to avoid anti-competitive contexts.

The reality is made even more complex by the inseparable intertwining between different areas of protection and respective control bodies, which modern interaction and exchange techniques create.

The individual sector regulations should interact in order to educate the individual, more and more often minors, to a correct and rational use of technological resources[23] taking into account the fact that not all personal data are provided directly by the subjects interested, but are sometimes extrapolated from the information disseminated on the web while browsing[24].

---

21 The Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 established the European electronic communications code, placing itself within the framework of the verification of the adequacy of the regulation (Regulatory Fitness-REFIT), which includes four directives, i.e. directives 2002/19 EC, 2002/20 EC, 2002/21 EC and 2002/22 EC, and regulation (EC) n. 1211/2009 of the European Parliament and of the Council. The directive conveys the regulation of the telecommunications, media and information technology sectors in a single European code, dedicating itself to the regulation of electronic communications networks and services, but not the contents of the same.

22 The European Commission has issued a Communication "Towards a common European data space" proposing a package of measures, "as an essential step towards a common data space in the EU, a seamless digital area, the scale of which allows development of new data-based products and services". COM (2018) 232, April 25, 2018.

23 See Italian law 29 maggio 2017, n. 71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyber bullismo". The legislation aims "*to combat the phenomenon of cyber bullying in all its manifestations, with preventive actions and with a strategy of attention, protection and education towards the minors involved, both in the position of the victims and in that of those responsible of offenses, ensuring the implementation of interventions without distinction of age in educational institutions*". In reality, worries and discomforts have an even wider scope that can also cross over into other types of criminally relevant offenses.

24 Personal data represent the resource on which the digital economy is based and the object of the right to data protection is recognized by Article 8 of the Charter of Fundamental Rights of the European Union. With a view to creating a European digital single market, Reg. (EU) 2016/679 of 27 April 2016 is placed on the protection of individuals with regard to the processing of personal data, as well as on the free movement of

Without denying the advantages produced by the diffusion of the internet and the affirmation of digital communication, it is obvious that the delicacy of the underlying interests requires careful and specific regulation. The positive results in terms of reduction of space and quality of communications cannot make us lose sight of the need to guarantee the correct use of information technologies.

2. Big data e antitrust.

The expansion of the digital economy has favored the growth of companies that own IT platforms and prompted the debate about the possible application of antitrust legislation in this sector.

The influence exerted by internet giants (Google, Facebook, Microsoft, Amazon) on market dynamics makes the reflection on the extent of the phenomenon topical.

The uncontrolled use of social networks and new technologies can lead to a real threat to regular competition.

The competitive structure leans in favor of the companies most able to collect and process users' data and information, with inevitable risks of closing the markets for less advanced companies.



The unscrupulousness that characterizes the so-called *digital era* and *big data*[25] raises a series of questions that embrace different, but interconnected areas: confidentiality, competition and consumer protection.

The data must be treated with respect for the privacy of the individual: any restrictions on access damage the ability of competitors to compete with consequent damage to consumers who, as the only interlocutors, will have the most technologically advanced companies, but not necessarily "best ".

The use of digital can be considered from a twofold perspective: positive if the innovative aspects and economic growth connected to it are valued, negative for the repercussions on the balance of the markets and the interests of users.

By favoring the first approach, the turning point marked by modern communication tools is evident, not only in terms of the quality of the products and / or services offered, but also in terms of efficiency and effectiveness of the systems of social interaction.

Companies take into account the preferences of those who use digital platforms and, therefore, are able to satisfy their needs. Recipients of products and services, in turn, should be able to find the most convenient offers more easily.

However, the risks that could arise from the uncontrolled use of telematic tools and the dominance exercised by some means of communication cannot be overlooked.

The only viable way, to scrutinize any abusive practices, is to evaluate, case by case, taking

such data and the Reg (EU) 2014/910 of the European Parliament and of the Council of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market.

[25] The image on the side is taken from *https://www.privacyitalia.eu/agcom-antitrust-e-garante-privacy-pubblicano-le-linee-guida-e-le-raccomandazioni-sui-big-data/11377/*.

into account not only the unfavorable effects on competition, but also the possible benefits[26] the conduct put in place by the companies suspected of illicit and avoid favoring parasitic behavior by the weakest contenders on the market.

Signs of anomalies in the functioning of competition do not necessarily arise from the holding of important positions, deservedly acquired, by the companies that are economically stronger and more difficult to emulate.

And this is where the antitrust paradox[27] is perceived: companies, whose competitive success derives from the use of greater skills and investments, risk being forced to share the fruits of their commitment with evident disincentives to improve products and services.

Most conducts likely to fall under the antitrust prohibition can complement the details of agreements, abuses or concentrations between companies[28].

The difficulty in identifying these types of offense is increased by the hybrid nature of the digital sector, which is still immature and difficult to classify, and postulates a wider conception of competition, that includes not only prices, but also innovation, quality, variety and the protection of personal data[29].

It is not yet clear how the infringements put in place on the online markets can be included in the schemes of the sector regulations on privacy and competition and which interests should be privileged in order not to frustrate the progress achieved.

The central point of the reflection is the choice of the method to follow: an autonomistic approach, aimed at a separate consideration of competition and privacy, or a combined approach, which privileges the plurioffensive nature of the personal data processing behaviors, but also the identification of the reference market and, more specifically, the consideration of a relevant data market distinct from that of online goods and services.

From the first point of view, there is no doubt that the digital world constitutes fertile ground for the perpetration of practices harmful to competition and privacy and it is important to understand whether the reference coordinates of the respective disciplines are sufficient to face abuses or should be integrated with new tools. To make the reference framework more complex is the observation that the free or negligible nature of the service

---

[26] See SC Salop, 'Exclusionary Conduct, Effect on Consumers, and the Flawed Profit-Sacrifice Standard, supra this issue' (2006) 73 Antitrust L.J. 311. See also G.J. Werden, 'Identifying Exclusionary Conduct Under Section 2: The "No Economic Sense" Test, supra this issue' (2006) 73 Antitrust L.J. 413.

[27] See R.H. Bork, *The Antitrust paradox: A Policy at War with Itself* (Basic Books 1978).

[28] It is useful to report the Google/DoubleClick case on 11 March 2008 DoubleClick, a company that provides internet services was acquired by Google, the most important search engine. The substantial amount of personal data held by the two companies has raised particular alarms with an invitation to the competent institutions, the Federal Trade Commission and the European Commission, to assess the privacy risks. Both bodies approved the transaction, flying over the possible interactions between Big data and privacy which, in reality, represented the most significant aspect of the controversy. See Google/DoubleClick, FTC File No. 071-0170, *Statement of federal Trade Commission* (Dec. 20, 2007), available at http//www.ftc.gov/os/caselist/0710170/071220 statement.pdf.; Case COMP/M.4731 - *Google/DoubleClick* (OJ 2008 C184/10). Another noteworthy story involved the two main social network Facebook e Whatsapp. platforms. In 2014 Facebook acquired Whatsapp for an amount of about 19 billion dollars. The doubts put forward in this hypothesis concerned the fate of personal information, until then correctly managed by Whatsapp, and now in the hands of a company with different powers and potential. In this case too, the FTC and the Commission authorized the merger without going into detail on the merits of the underlying issues. A few years later, Facebook's note to the Commission of "admission of guilt" about the incorrectness of the information transmitted to explain the pairing of the user profiles of the two platforms, led to the imposition of two fines of € 55 million each. See *Complaint, Request for Investigation, Injunction, and Other Relief, Electronic Privacy Information Center, Center for Digital Democray, In re Whatsapp, Inc.* (March 6, 2014), available at http //www.centerfordigitaldemocracy.org/sites/default/files/Whatsapp%20 Complaint.pdf.; Case COMP/M. 7217, *Facebook/ Whatsapp,* OJ C(2014) 7239 final.

[29] See A Giannaccari, 'La storia dei Big Data' (13) 322.

provided by the users of the platforms does not reconcile with the need for antitrust intervention.

The impact of modern social interaction tools has led individual national and European authorities to a no longer postponable assessment of the extent of the phenomenon and its application consequences, opting, on the one hand, for the application of the principles and rules on competition , on the other hand, for the search for more effective and innovative enforcement criteria in view of the resolution of the most controversial aspects relating to confidentiality, the result of the forced coexistence between apparently antithetical areas (privacy and competition)[30].

In a constantly evolving society, driven by the incessant advancement of increasingly sophisticated technologies, even the sector rules no longer adequate to a complex and changing reality risk remaining a dead letter; this leads to favoring non-isolated intervention tools, which take into account the peculiarities of the institutions involved.

With regard to the market to be taken as the object of analysis (if that of data as a market distinct from that of goods and services), identification is made difficult in a little-known context such as the digital one.

To this end, it is appropriate to establish whether the data represent a mere production input or the output of the activity itself in the different markets in which the company operates and to ascertain the degree of substitutability of the data..

The only certainty is that users, by making available, knowingly or unknowingly, the information concerning them, themselves become an evaluation parameter of the market power of companies, an alternative to the traditional one based on quotas and turnover[31].

The particularity of the service provided by the users of the platforms (the entry of their personal data), not strictly economic, but susceptible to economic evaluation, allows telematic companies not only to acquire or increase their market power, but also to easily evade antitrust controls: once transmitted, the data escape from the sphere of users and the latter are not able to hinder its dissemination[32]. From this point of view, a synergistic consideration of competition and privacy appears to be the preferable solution to face and stem the disruptive impact that characterizes the activity of collecting and processing the data themselves.

3. Binding practices and leverage theory in the digital age.

The interaction between competition and digitization in the context of the virtual market, due to the potential for transformation that characterizes it, requires special attention. The affirmation of business models, based on the collection and processing of data, has given a strategic role to leading companies in the sector, more able to recognize the preferences and habits of users, and faster in offering products and / or services satisfactory to the relative needs. Among the offenses that arouse particular alarm, due to the repercussions in terms of competitive equilibrium, there is the attempt of the giants on the net to extend their power

[30] See reports: *Big data and differential pricing*, by The Executive Office of the President of the US, February 2015, available at http://obamawhitehouse.archive.gov; *UK Competition & Markets Authority Report* (CMA38, June 2015)*, The commercial use of consumer data*, in www.gov.uk; *Big Risks, Big Opportunities: the Intersection of Big Data and Civil Rights*, White House Report, 4th May 2016; US Federal Trade Commission Report (January 2016), *Big Data. A tool for Iclusion or Exclusion?*, at www.ftc.gov.

[31] See M Meriani, 'Digital platform and spectrum of data protection in competition law analyses' (2017) 38 (2) ECLR 89.

[32] Four types of activities can be distinguished that are likely to cause damage to privacy: 1) collection of information, 2) processing of the same to derive useful insights, 3) dissemination of information and insights themselves, 4) influence of interested parties based on information and to the insights gained. See DJ Solove, 'A Taxanomy of Privacy' (2006) 154 U. Pa. L. Rev. 477.

in adjacent markets. For example, Internet Explorer users that visit Google's home page see the Google Chrome installation on the right:



The driving force of the phenomenon is usually found in the *leverage theory* or theory of *leverage*, elaborated by the North American doctrine: the company uses its market power over a given asset (the tying product) as a lever to acquire a competitive advantage on the market of a well distinct (the tied product)[33]. This leads to an alteration of the competition in the tied product market: consumers will choose the tied good to access the binding good, rather than for the best quality and / or the cheapest price[34].

The legal-economic analysis makes it possible to combine well-rooted concepts and categories in this sector with the uncertainty and gaps that characterize the online markets.

In the 1950s, Chicago School economists challenged the theoretical foundations of the doctrine of leverage, of the unlawfulness per se of joint selling and vertical integrations [35]. Regarding the theory of the decisive leverage is the intuition of the School, according to which "a monopolist could not earn additional monopoly profits in an adjacent market by leveraging into it (the" single monopoly profit theorem ")[36]

In other words, the monopolist through bundling does not increase its market power, since the amount of profits obtained in the tied product market will be deducted in equal measure to that made in the bond product market.

---

[33] For a description of the phenomenon, albeit with critical insights, see RA Posner, 'Exclusionary Practices and the Antitrust Laws', 41 University of Chicago Law Review 508 (1974): "*People used to regard tying as a method by which a firm having a monopoly in one market (for example computers) could obtain a monopoly of a second product (such as computer punch cards) by requiring all purchasers of the first product also to buy the second from it*".

[34]It has been demonstrated - and paradoxically by a Chicago author, Ward Bowman - that leverage is possible when the two goods (or the combination of goods and services) are used in varying proportions. When, however, used goods in fixed proportions are sold for free or even, predatory, below cost, it is inevitable that the antitrust analysis profiles are examined in a dynamic perspective on which the (static) price theory can say little or almost nothing. With this in mind, the repression of the tying of the Windows operating system to the Internet Explorer program for web browsing in the famous Microsoft case was deemed illegal monopolization on both sides of the Atlantic (*United States v. Microsoft Corp*, 147 F.3d 935, D.C. Cir. 1998).

[35] Throughout the 20th century, the Supreme Court held vertical practices, such as bundling agreements per se, on the assumption that the monopolist, in a given market, was using the tying strategy to extend its power from the binding product market to the market. related product market. See *Carbice Corp. v. American Patents Development Corp.*, 283 U.S. 27 (1931).

[36] H Hovenkamp, *The Antitrust Enterprise: Principle and Execution* (Harvard University Press 2008) 34; A Director - EH Levi, *Law and the Future: Trade Regulation* (1956) 51 Nw. U. L. Rev. 281.

Tying, following the Chicago line of reasoning, is not an expedient to obtain double monopoly profits and hinder competition in the tied product market[37]. Vertical integration and the leverage effect are driven by efficiency, in terms of higher quality or lower prices, and therefore legally considered valid, as a source of benefits for consumers.

Although criticized, the Chicago School's approach is valuable and current for understanding the unfolding of antitrust offenses in the intricate digital scenario.

The theoretical insights offered, far from denying the validity of the theory of leverage, suggest a distinction, neglected in the past by the Courts, between pro and anti-competitive leverage depending, respectively, on the positive or negative effects on regular competition.

If in the context of digital platforms it appears difficult for the owners, whose behavior is subjected to antitrust scrutiny, the demonstration of efficiencies becomes relevant proof of possession of greater skills and / or the implementation of investments compared to competitors.

By applying an adequate standard of consumer welfare, which pays due importance to the justifications put forward by suspects of wrongdoing, it is not difficult to scrutinize the hypotheses likely to fall within the meshes of antitrust repression.

The idea of adopting remedies aimed at structural separation, which limits the ability of dominant platforms to hinder competition by offering additional services[38], contributes to enriching and making the reference framework more interesting.

A solution of this type, if it prevents the abusive exploitation of the dominant position by leading companies in the digital market, avoiding situations of conflict of interest with respect to competitors, undermines the conducts of positive financial leverage with the inevitable repeal of the consumer welfare standard so dear to antitrust doctrine[39].

The theoretical approach, attributable to the principle of "non-discrimination" or "platform neutrality[40], according to which platform owners should not be allowed to obtain advantages over their adjacent products, exploiting the size and prestige they enjoy in the platforms themselves, it overlooks the possibility that leveraging behavior can have positive effects for competition and sacrifices the parameter of consumer well-being, a fundamental purpose of anti-monopoly laws[41].

Recently, the European Union report on digital competition [42] highlighted how the Commission cares about the well-being of consumers and the prevention of damage to them:

---

[37] See A Cucinotta, 'The antimonopoly regime of the tying clauses', in *Quadrimestre*, 1993, 90. The author clarifies whether "*the tie-in cannot function as a monopoly creating device, this deduction does not seem to authorize definitive conclusions about the absolute inadmissibility of the idea of leverage*". In fact, in the case of complementary products used jointly in variable proportions, leverage actually operates and, therefore, the monopoly power increases and determines the realization of higher profits than those that would derive from a single product.

[38] See LM Khan, 'Sources of Tech Platform Power' (2018) 2 Geo. L. Tech. Rev. 325, 332.

[39] See MH Riordan, *Competitive Effects of Vertical Integration*, in *Handbook of Antitrust Economics* 48 (Paolo Buccirossi ed., 2008); *Global Antitrust Institute, Competition and Consumer Protections in the 21st Century, Vertical Mergers*: Hearing Before the Fed. Trade Comm'n (2018).

[40] See K Caves, H Singer, 'When the Econometrician Shrugged: Identifying and Plugging Gaps in the Consumer Welfare Standard' (2019) 26 Geo. Mason L. Rev.; FA Pasquale, 'Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines' (2008) U. Chi. Legal F. 263; FA Pasquale, 'Dominant Search Engines: An Essential Cultural & Political Facility', in B Szoka, A Marcus (eds.), *The Next Digital Decade: Essays on the Future of the Internet* (TechFreedom 2010), 399.

[41] Applying the principle of non-discrimination to platform owners would be prevented from offering users the advantages of new features in the platform code. See PF Todd, 'Digital Platform and the Leverage Problem' (2019) 98 Nebraska Law Review 486.

[42] Competition policy report - annual report 2019 (2019/2131 INI). See also J Cremer, YA de Montjoye and H Schweitzer, *Competition Policy for the Digital Era*, Eur. Comm'n, 1, 42 (2019); Stigler Center, *Committee for the Study of Digital Platforms*, *Market Structure and Antitrust Subcomm Committee*, Report 77 (2019).

the pursuit of these objectives, especially in digital markets, requires a more which includes the new approach which consists in considering data protection as a quality criterion when assessing the impact of mergers on consumer welfare (para. 16 p. 42)[43].

The foregoing observations highlight the state of the art on the issues dealt with without being able to provide definitive answers that only time and the evaluation of individual concrete cases can offer.

What is certain is that, even in an immature and unexplored context such as the digital one, the synergy between economics and law, very influential in recent decades for the understanding and regulation of antitrust offenses, becomes an effective tool for understanding exact scope of the institutions involved and respond to the underlying protection needs.

Conclusions.

The issues addressed turn out to be even more suggestive in a moment, like the current one, of closure and social distancing for the coronavirus pandemic.

The need to contain the number of infections has made the use of digital tools not only indispensable, but also exclusive to carry out most of the work, professional, educational and commercial activities.

Smart working and distance learning have represented a valid alternative to work and face-to-face teaching, despite the difficulties associated with the impossibility of equating the results.

The massive spread of the epidemic has brought the whole world to its knees: technological progress and multimedia communication tools have made it possible to alleviate damage, contain losses and reduce interpersonal distances.

In the commercial sector, the practice of proceeding with online purchases for countless categories of products and services had already been established for some time, now further rooted as a result of the COVID emergency.

Store chains with medium and high quality Italian and international brands have adopted the so-called on demand sales: through whatsapp, customers interact with a personal shopper asking for information or sending images until the purchase deed is completed. This system will be able to convert even the laziest, or less experienced, to digital shopping, and those who, due to lack of time, give up the purchases of goods that are not essential and will certainly find widespread diffusion in other commercial areas as well.

These ways of perfecting commercial relationships undoubtedly mark a new phase in the path that characterized the birth of the internet and the digital age, attracting users and influencing their preferences.

This trend must be managed and monitored to ensure the correct use of resources and protect potential buyers from abusive behavior whose consequences could reverberate on several fronts: privacy, competition, authenticity and originality of the products purchased. Buyers who, even if considered weak subjects and in a relationship of information asymmetry with producers and / or sellers, take on the role of protagonists within the reference contexts.

This leads, by shifting attention to the legal-economic side, to a rethinking in the antitrust field of the existing opinion of the Court of Justice which, in defining the abuse of a dominant position as a situation of economic power thanks to which the company is able to maintain independent behaviors also towards consumers, he neglected the importance that the latter would soon have in market dynamics[44].

---

[43] The report assumes the merger between Facebook and Whatsapp as an example, suggesting that the Commission request a prior informal declaration for the concentrations that are concluded within the markets.
[44] Corte giust., 13 febbraio 1979, C-85/76, *Hoffmann-La Roche & Co.*, in *Racc.* 1979, 461.

With a view to complementary protection aimed at guaranteeing the right balance between the achievement of a high level of consumer protection and the promotion of the competitiveness of businesses, the EU directive 2019/770 of 20/05/2019, on the subject of contracts of digital supply and digital services, and the EU directive 2019/771 of 20/05/2019, on the subject of contracts for the sale of goods, both oriented towards maximum harmonization.

If in the economic language the market is the ideal place where the demand and supply of a good or a service meet, today, in the digital age, the market becomes the "real or virtual" place where the meeting between supply and demand and the negotiations that precede the conclusion of the deal.

It is clear that we are now facing a situation of no return: the multimedia world represents a reality and, today more than ever, in this moment of discomfort and crisis due to the COVID emergency, we realize the advantages and disadvantages. connected to the phenomenon.

Sharing preferences, passions and behaviors creates a sort of psychological dependence not only between the subjects involved in communication, but also between the "contacts" who observe, comment on and imitate the choices of behavior and purchase (the so-called social shopping).

The hope is that common sense and respect for the fundamental rights of the person will prevail and that the original role that inspired their invention will be restored to electronic instruments, that is, of aid and not a substitute for the human mind.

Given the positive effects of the digital revolution, the detrimental consequences on competition and consumer protection in general cannot be overlooked.

There remains a feeling of concern for the future: the way of acting of each of us will become impersonal and objective and in order to govern the technique, we will end up being governed by it.

Achieving the maximum of goals, with the minimum use of means, becomes the only way of thinking.

The progress marked by multimedia means is undoubted, but it should be diligently used so as not to sacrifice the individual as a person.

In this coronavirus season that seems not to end, the perplexities are heightened. The use of IT and digital tools becomes the exclusive vehicle for information and communication with the inevitable aggravation of situations of dependence, marginalization and isolation.

It is premature to ask whether the current regulations will be able to offer adequate protection that embraces privacy, competition and the interests of consumers, a question destined to animate the debate for a long time to come, but the certain data from which to start is based on the idea of protection. of personal data as a right and natural development of the right to privacy.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Model of liability for harm caused to the patient by the use of bioprinting technologies: view into the future[1]

DMITRY E. BOGDANOV[2]
Professor at the Kutafin Moscow State Law University (Russia)

Abstract

The rapid development of bioprinting technology creates serious challenges for the legal system, which is lagging behind scientific and technological progress in its development. Lawmakers and the judicial system will soon be forced to answer the questions posed by the new technological revolution. The main area of legal regulation that bioprinting will have a serious impact on is tort liability, since the use of this technology will be associated with harm to the health of patients.

There is a question about the rules that will need to be followed when compensating for harm to the patient. The article considers various models of liability for harm to the patient caused by the use of bioprinting technologies. It is concluded that the patient's voluntary informed consent to treatment using bioprinting technologies can be qualified as the patient's acceptance of the risk of possible adverse consequences that are beyond the control of the medical organization. Such consent may be qualified as a circumstance that is the basis for releasing a hospital from liability for harm caused to a patient when using bioprinting technologies.

Keywords: 3D printing technology - Three-dimensional bioprinting - Tort – Harm - Product liability - Fault liability - Non-fault liability.

Summary: Introduction. – 1. Current practice of compensation for damage caused by 3D medical products. – 2. Modern approaches to determining the model of liability for harm caused to the patient by the use of bioprinting technologies. – 3. Prognostic view of the model of liability for harm caused to the patient by the use of bioprinting technologies. – 4. Concluding remarks and future perspectives.

Introduction

Currently, the world is facing the rapidly developing 3D printing technology designated in scientific literature as an example of additive technology[3]. This technology is based on the connectivity method, which essence lies in the fact that a 3D printer through serial connection and layering of "ingredients" (powders, metal, polymers, etc.) ensures layer-by-layer printing of a new three-dimensional object. 3D printer operation is controlled by a

[1] This study was financially supported by the Russian Foundation for Basic Research within the framework of the Scientific Project No. 18-29-14027 mk "Concept of legal regulation of relations for conducting genomic research in creation and use of bioprinted human organs".

[2] Doctor of Law, Professor, Department of Civil Law, Kutafin Moscow State Law University (MSAL) 9, Sadovaya-Kudrinskaya st., Moscow, 125933, Russia
ORCID: 0000-0002-9740-9923
ResearcherID: P-9117-2015
E-mail: Bogdanov.de@yandex.ru

[3] E. J. Kennedy and A. Giampetro-Meyer, 'Gearing Up for the Next Industrial Revolution: 3D Printing, Home-Based Factories, and Modes of Social Contro'l, 46 (4) Loyola University Chicago Law Journal, 955-988 (2015).

computer with appropriate software; however, the printing itself is preceded by creation of a computer-aided model (prototype) of the future three-dimensional object (Computer Aided Design files or CAD files), which could be obtained, for example, by means of three-dimensional scanning.

3D printing technology development leads to "digitalization" of the material world objects, boundaries between the physical world and the digital space are being erased, since distinction between a computer-aided prototype and its material embodiment is thinned to one click[4]. As noted by Lucas Osbourne, 3D printing is becoming the reason for overlaying worlds of atoms and bits on each other. With the spread and improvement in 3D printing technology, three-dimensional computer-aided templates for many products would become equivalent to their physical counterparts. Regulating relations associated with such files would appear to be a major challenge for the legal system seeking to adapt to the world of 3D printing[5].

If three-dimensional printing (3D printing) digitalizes objects of the material world, which relates not only to high-tech products (for example, components and parts of spacecraft or aircraft), but also to everyday goods (for example, dishes or shoes), then bioprinting starts to digitalize a person and his body. Subsequently, this could lead to a kind of digitalizing the very existence of a person[6], since it would directly depend on its digital embodiment in the corresponding CAD files, i.e. electronic templates both of the entire human body, as well as of its separate parts, individual tissues and organs.

Currently, 3D printing technology is already actively introduced in the area connected to a person "digitalization" for health purposes. Thus, a number of corporations (for example, Organovo, Aspect Biosystems, TeVido Biodevices) are successfully developing the bioprinting technology for liver tissue and other human organs in order to provide toxicological testing of new medical preparations, which helps to reduce risks of harm, as well as time required for testing new medical prescriptions and expenses related with this. 3D printing is actively used in patients' recreation after suffering serious injuries, since this technology makes it possible to print individual prostheses and implants that consider individual physiological characteristics of each patient. Three-dimensional printing also makes it possible to restore the patient's appearance, as it is already actively used in face surgery. 3D printing is used in many leading medical centers before complex operations, which technique was initially practiced on a 3D model of the corresponding organ, for example, before transplantation[7]. Back in 2018, Roscosmos State Corporation, INVITRO and 3D Bioprinting Solutions announced successful completion of the first stage of the Magnetic 3D-Bioprinter space experiment conducted on board the International Space Station (ISS). For the first time in space, human cartilaginous tissue and thyroid gland of a rodent were printed.

But most importantly, bioprinting is aimed at creating a new medical paradigm that would ensure overcoming the deficit of human organs and tissues in transplantology. Since, the global problem is the constant increase in the number of patients requiring spare-part surgery and the acute shortage of donor organs necessary for transplantation.

Legal literature is trying to formulate definition of this technology; thus, Jasper Tran

[4] D. H. Brean, 'Patent Enforcement in Cyberterritories', 40 (6) Cardozo Law Review, 2549-2596 (2019).
[5] L. Osborn, 'Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms', 51 San Diego Law Review, 553-621 (2014).
[6] J. Tran, 'To Bioprint or Not to Bioprint', 17 (1) North Carolina Journal of Law and Technology, 123-178 (2015).
[7] M. Varkey and A. Atala, 'Organ Bioprinting: A Closer Look at Ethics and Policies', Wake Forest Journal of Law & Policy, 5 (2), 275-298 (2015).

indicates that bioprinting is production or manufacture of a living organism using the ink made from living cells[8].

Serious challenge to bioprinting technology is advanced by creating a replica of the human organ "frame" repeating complex architecture, on which several types of living human cells would be layered during the three-dimensional bioprinting. Thus, human organ frame creation (3D printing) is of utmost importance for bioprinting, since growth and division of living human cells would be taking place on it.

Bioprinting technology is able to revolutionize medicine, but this technology also poses serious risks[9], as we still are unable to imagine the entire picture of consequences and problems that will arise in connection with active introduction of this technology[10].

If harm to the patient's life or health is caused by drawbacks of computer-aided design in creating a digital model (replica) of a human organ or of this organ frame, the question arises on the rules that should be followed when compensating the patient for harm. Scientific literature directly indicates that tort liability is one of the main areas of legal regulation, which would be seriously influenced by 3D printing[11]. This predestinates the need in special studies aimed at determining models of liability for harm caused in the additive technologies.

1. Current practice of compensation for damage caused by 3D medical products.

As of today, court practice related to the issues of compensation for harm caused to the patients' life or health when using bioprinting technology is missing, since this is a technology of future, but of the near future. According to forecasts, human heart effective bioprinting is expected in the next 15-20 years. At present, bioprinting of individual human tissues, blood vessels, etc. is already underway.

However, there is already certain court practice on issues related to compensation for harm caused by defective medical devices, implants, etc., made using the 3D printing (additive technologies). Thus, judgement in the Buckley v. Align Tech., Inc.[12] case examined a patient's lawsuit against the dental mouthguard producer, the device was individually manufactured using the 3D printing technology. The patient was not in direct contractual relationship with the producer of this medical product. It was manufactured by the dentist order to eliminate occlusion. The patient was referring to the fact that producer advertising his medical products manufactured using the 3D printing technology misled her and other consumers that his product could eliminate occlusion.

The court rejected the lawsuit basing on the intermediary liability doctrine (intermediary doctrine). Plaintiff's arguments that producer was obliged to carry out medical analysis of the dental prints for individual medical product 3D printing and, therefore, was obliged to warn the patient about consequences of using the dental mouthguard. Based on the intermediary doctrine, the court indicated that medical product was prescribed by a dentist and was manufactured to order by the producer, who was not a medical expert. The defendant was obliged to warn the dentist of any dangerous side effect, but he did not have a similar obligation with respect to the plaintiff.

Thus, the patient was rejected in this case with the suit for compensation for health harm

---

[8] J. Tran, n 6 above, 125.

[9] M. H. Park, 'For a New Heart, Just Click Print: The Effect on Medical and Product Liability from 3D Printing Organ', 4 University of Illinois Journal of Law, Technology & Policy, 187-199 (2015).

[10] E. Lindenfeld, '3D Printing of Medical Devices: CAD Designers as the Most Realistic Target for Strict, Product Liability Lawsuits', 85 (1) University of Missouri-Kansas City Law Review, 79-103 (2016).

[11] G.Howells and C. Twigg-Flesner and C. Willett, 'Protecting the Values of Consumer Law in the Digital Economy: The Case of 3D-Printing', in A. De Franceschi and R. Schulze (eds), Digital Revolution - Challenges for Law (Beck, 2019), 214-244 .

[12] Buckley v. Align Tech., Inc., No. 5:13-CV-02812-EJD, 2015 WL 5698751 (N.D. Cal. Sept 29, 2015)

caused by a medical product made using the 3D printing technology. Motives for lawsuit rejection reflect the peculiar approaches in tort law characteristic for the Common Law countries. It looks like rejection of the lawsuit, even for the American law, is far-fetched in spite of using the intermediary doctrine. Since harm was caused by a medical product that should be safe for any end-user, regardless of whether such user was in a contractual relationship with product manufacturer. The fact that there was an intermediary between producer and consumer in the form of a doctor (medical organization) does not deprive a damaged person of the right to be compensated for harm under such circumstances.

It should be noted that the rules of Product Liability Directive 85/374/EEC[13], the Civil Code of Russia and the Tort Liability Law of the PRC allow in similar situations to impose liability for harm compensation on the medical device producer.

Given this decision, several authors believe that 3D printing connected to using individual computer-aided data (CAD files) obtained by scanning patients for the three-dimensional printing of medical devices blurs the boundaries between professional medical services (treatment) and individualized production creating the basis for the intermediary liability doctrine[14].

In another case (Cristian v. Minn Mining & Mfg. Co[15]), involving compensation for harm by defects in a breast implant, the court indicated that the person, who developed the breast implant model, could not be held strictly liable for harm caused by the product, because he did not participate in the production process. Thus, the court limited the product liability for defective goods establishing that only the direct manufacturer should bear strict responsibility for the defective goods, but not the developer (designer, planner) of the given product model.

Richard Rubenstein in this regard points out that the US case law establishes that strict liability rules for structural defects in regard to implantable medical devices are not applicable due to legal policy reasons. He asks a question about fairness of complete prohibition on application of rules governing strict liability for design (engineering) defects in regard to the 3D printed implants, where the process of computer-aided model design (CAD files) makes it possible to change the product structure for each individual patient. However, the author himself points out inability to answer this question, as the modern system of legal regulation is designed to regulate relations connected to mass production of traditional medical devices[16].

Examples provided from law enforcement practices indicate a problem in determining the model of liability for harm caused by additive technologies, in general, and bioprinting, in particular.

2. Modern approaches to determining the model of liability for harm caused to the patient by the use of bioprinting technologies.

Modern literature is already taking attempts to elaborate a scientific response to new technological challenges forcing to rethink the tort liability concept. So, Jamil Ammar thinks

---

[13] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210.

[14] J.M. Beck and M.D. Jacobson, '3D Printing: What Could Happen to Products Liability When Users (and Everyone Else in Between) Become Manufacturers', 18 Minnesota Journal of Law, Science & Technology, 143-205 (2017).

[15] Cristian v. Minn Mining & Mfg. Co 126 F. Supp. 2d 951, 959 (D. Md. 2d 1096, 1117 (D. Ariz. 2003)

[16] R.H. Rubenstein, '3D Printed Medical Implants: Should Laws and Regulations Be Revolutionized to Address This Revolutionary Customized Technology', 7 (349) NATIONAL LAW REVIEW, (2017) available at https://www.natlawreview.com/article/3d-printed-medical-implants-should-laws-and-regulations-be-revolutionized-to-address (last visited 10 June 2020)

that in order to compensate for harm to a patient health caused by using the bioprinting technologies, it is possible to use three theories (approaches) in the liability area:

1) medical malpractice based on a guilt special delict;
2) violation of the contract warranty;
3) strict liability imposed regardless of the delinquent non-fault liability[17].

However, as the indicated author points out, none of these theories completely suits the situations involving harm due to drawbacks in computer-aided design of the human organ three-dimensional models (CAD-Files)[18].

Thus, strict liability imposed regardless of the delinquent guilt in American law is possible only in case of compensation for harm caused by defective goods (product liability)[19].

Scientific literature notes that over the latest time a global trend in product liability is establishment of strict (non-fault) standard for such liability[20]. Therefore, non-fault strict standard of liability for harm caused by defective goods is provided, for example, in Article 1 Product Liability Directive 85/374/EEC, Article 1095 of the Civil Code of Russia, Article 41 of the PRC Tort Liability Law 2010[21].

However, the literature indicates that mass tragedies are becoming the trigger for development of legislation in product liability. It was the lack of effective remedies in situations of massive harm to the health of exposed people by a particular product that led to establishment of strict non-fault liability for harm caused by low-quality goods. Thus, Kristie Thomas claims that it was the "melamine scandal" that provoked inclusion in the new PRC Tort Liability Law rules detailing strict manufacturer liability for harm caused by defective goods. This scandal reminds of the crisis situation in product liability that occurred in Europe in 1960-1970 as a result of the so-called "thalidomide catastrophe", which subsequently affected adoption of the Product Liability Directive 85/374/EEC[22].

It also appears of interest that the US courts are following similar logic, as a rule, applying the rules on strict liability only in situations of causing harm by mass product torts[23]. Despite the fact that the "mass character" indicator is not provided as a prerequisite for establishing strict liability in the Restatement (Second) of Torts, scientific literature indicates creation of incentives for ensuring safety and distribution of risks as goals for such liability[24].

The literature also notes that the US courts are reluctant to extend the scope of strict liability upon defective products (product liability) to software (computer programs), since software is generally considered as a service, but not a product[25]. For comparison, the standard of strict non-fault liability in Russian law covers harm caused not only by defective goods, but also by works and services (Article 1095 of the Civil Code of the Russian Federation).

To illustrate the US court approach, judgement in the Sanders v. Acclaim Entm't case[26]

---

[17] J. Ammar, 'Defective Computer-Aided Design Software Liability in 3D Bioprinted Human Organ Equivalents', 35 (3) Santa Clara High Technology Law Journal, 37-67 (2019).
[18] Ibid 39-42.
[19] N. D. Berkowitz, 'Strict Liability for Individuals? The Impact of 3-D Printing on Products Liability Law', 92 (4) Washington University Law Review, 1019-1053 (2015).
[20] G. Brüggemeier, *Modernizing Civil Liability Law in Europe, China, Brazil and Russia: Texts and Commentaries* (Cambridge University Press 2011) 10.
[21] K. Thomas, 'The Product Liability System in China: Recent Changes and Prospects', 63 (3) International & Comparative Law Quarterly, 755-775 (2014).
[22] Ibid 757-762.
[23] J.K. Gable, 'An Overview of the Legal Liabilities Facing Manufactures of Medical Information Systems', 5 Quinnipiac Health Law Journal, 127-147 (2001)
[24] E. Lindenfeld, n 10 above, 82-85.
[25] J. Ammar, n 14 above, 42-43.
[26] Sanders v. Acclaim Entm't, 188 F.Supp.2d 1264 (D. Colo. 2002)

could be considered, in which the court indicated that computer games were not a "product" for the product liability purposes. Similar conclusion was made by the court in the judgment in the Wilson v. Midway Games Inc. case[27] considering the virtual reality technology. It is worth examining court position in the James v. Meow Media, Inc. case[28], where the court took a differentiated approach indicating that software could be considered as tangible property for tax purposes and as a product in relation to the Uniform Commercial Code (UCC) objectives, but this did not mean that intangible thoughts, ideas and messages contained in computer video games, video files or online materials should be considered as products for the purpose of imposing strict liability. Thus, activities of software developers and website operators are not connected to "products".

It could be stated that North American courts are taking conservative approach in regard to the "product" definition relating to the question of admissibility of imposing the non-fault liability according to the product liability model.

It is of interest that the Australian law belonging together with the North American law to the Common Law system considers software as a "product" for the purpose of imposing strict non-fault liability under the defective product liability model[29].

Similarly, the US law enforcement practice addresses the problem of liability for harm caused by provision of medical services. Given that patients are receiving treatment services in hospitals, and activities of medical organizations, as a rule, are not connected to selling the products, the courts refuse to compensate harm caused to the patient according to the strict non-fault liability model (Perlmutter v. Beth David Hospital[30]). Product liability model for harm caused by a defective product does not cover such relations[31]; compensation for harm is carried out according to the model of special guilty tort (medical malpractice). It is noted in practice that any arguments in favor of establishing a strict standard of responsibility for medical organizations are outweighed by the generally useful nature of their activities related to saving lives and human health (Cafazzo v. Cent. Med. Health Servs., Inc.[32]) Thus, in one case, the court indicated that medical services are often experimental in nature, and when provided, certainty in result is missing, since it depends on factors beyond the control of a professional. Medical services are necessary for society and should be accessible for people (Hoven v. Kelble[33]).

Jamil Ammar in this regard indicates that the bioprinting specificity is associated with combining "products" and "services", it is difficult in this area to differentiate activities of developers specializing in software used to create digital models (CAD files) of human organ analogues, as well as activities of medical organizations and manufacturers of medical devices. Taking into consideration that computer-aided design plays a key role in bioprinting, the author believes that it is easier and cheaper to prevent harm to the patient health even at the stage of creating a human organ digital model imposing strict non-fault liability on the person performing such computer-aided design of a human organ. In this case, it is necessary to differentiate two groups of tortfeasors: first, medical organizations independently carrying out activities in bioprinting and controlling the process of human organs bioprinting; second, developers of software for creating computer-aided models of human organs (CAD files)

---

27 Wilson v. Midway Games, Inc., 198 F.Supp.2d 167, 173 (D. Conn. 2002)

28 James v. Meow Media, Inc., 90 F.Supp.2d 798, 810 (W.D. Ky. 2000)

29 J. Nielsen and L. Griggs, 'Allocating risk and liability for defective 3D printed products: product safety, negligence or something new?', 42 (3) Monash University Law Review,712-739 (2017).

30 Perlmutter v. Beth David Hospital, 123 N. E. 2d 792, 795 (N.Y. 1954)

31 J. Ammar, n 14 above, 46-47.

32 Cafazzo v. Cent. Medical Health Services, 668 A.2d 521 (Pa. 1995)

33 Hoven v. Kelble, 256 N.W.2d 379 (Wis. 1977)

used in bioprinting[34].

It should be noted that earlier Eric Lindenfeld also pointed out the need to differentiate liability of developers of human organs computer-aided models (CAD files), who should be strictly liable regardless of their guilt and of responsibility of medical organizations and 3D printers manufacturers, which, in his opinion, should be liable according to the culpable standard[35].

Another point to be made here is that in the US law enforcement practice the germs of a new approach are already visible allowing software qualification as a product in order to impose strict (non-fault) liability on its developers. Thus, judgement in the Corley v. Stryker Corp. case[36] is of interest for our study, as it addressed the issue of manufacturing a surgical disposable cutting guide, which was subsequently used in operating the patient. This guide was created using software based on a three-dimensional model (3D model) taking into account the patient individual anatomy. In this case, the court agreed with the plaintiff's claim that the software was defective, because in its design the cutting guide used during the operation was "unreasonably dangerous due to alleged software defects".

However, Jamil Ammar points out that introducing strict non-fault liability could be avoided by using the unavoidably unsafe product defense rule, which could possibly be applied to liability in bioprinting[37].

This rule is provided for in Paragraph 402A of the Restatement (Second) of Torts, which states that certain products may not be completely safe in their intended or normal use. The seller of such products is not strictly (non-fault) liable for their use adverse consequences. It is noted in literature that this rule is usually not applied to production, but to design drawbacks of a product, when a safer product design solution is missing[38].

As a result of studying the North American experience in tort liability, Jamil Ammar concluded that the standard of strict non-fault liability and the guilty standard are not fully applicable to torts in bioprinting, since the strict liability standard for developers of software used to create computer-aided models of human organs (CAD-Files) could increase security of such software, but reduce its effectiveness. The liability guilty standard is complicated by the need to prove the tortfeasor negligent delinquency. Therefore, the author proposes a third approach imposing liability on developers of defective software used in computer-aided modeling of human organs. This approach is based not on artificial distinction between products and services, but on differentiating the services rendered into administrative (technical) and proper medical services. Accordingly, strict non-fault liability should be assigned only for harm caused in provision of technical services. However, the author is not proposing criteria for separating these services; he believes that the nature of a service should be determined by the court in each specific dispute, i.e. ad-hoc differentiation. In his opinion, imposing strict non-fault liability on software developers and persons engaged in the development of computer-aided models of human organs (CAD files) is economically justified, because it makes it possible to prevent tort in bioprinting at the initial technological stage and at minimal cost[39].

The source of inspiration for Jamil Ammar in elaborating the approach based on differentiating services between "technical" and proper "medical" services was to separate court decisions, where, in order to impose non-fault liability on a medical organization, the

---

[34] J. Ammar, n 14 above, 37-67.
[35] E. Lindenfeld, n 10 above, 79-103.
[36] Corley v. Stryker Corp., 2014 WL 3375596 *1 (W.D. La. May 27, 2014)
[37] J. Ammar, n 14 above, 37-67.
[38] K. Thomas, n 19 above, 755-775.
[39] J. Ammar, n 14 above, 37-67.

court indicated a different (non-medical) nature of the service provided (Johnson v. Sears, Roebuck & Co.[40]).

Of course, disadvantage of this approach lies in the lack of a clear criterion for differentiating services between medical and technical. For example, there appears a question, whether technical or medical service would include processing data obtained on the basis of a patient computer tomography followed by its subsequent use in creating a three-dimensional model of a human organ and directly in the bioprinting. According to the author's logic, the court would have to answer this question, each time separately assessing circumstances on the case.

Scientific position is of interest, according to which developers of computer-aided models of medical devices (computer-aided designers) should be imposed with strict non-fault liability, and medical organizations should only be liable, if there is fault (negligence); this idea was also presented by other scientists. Moreover, Eric Lindenfeld expressly points out that even a minor mistake in the computer-aided design of medical devices could lead to fatal consequences; therefore, computer-aided model developers should be held liable regardless of their fault[41].

It is obvious that computer-aided design of a three-dimensional model of the bioprinted organ, as a rule, would be carried out not by the third-party companies, but directly by those medical organizations obtaining appropriate equipment and qualified personnel. Therefore, if the indicated scientific position is followed, there appears the need to differentiate the liability model of a medical organization depending on its type of activity, i.e. technical (computer-aided) preparation to bioprinting and proper medical activity connected to patient treatment using the bioprinted organ transplantation. If any defect is identified in the bioprinted organ computer-aided design, i.e. in the computer-aided replica content (CAD files) of the bioprinted organ, liability for the harm caused should occur regardless of the medical organization fault.

With regard to elaborating the medical organization liability model for harm caused to the patients' life or health, including that associated with using the bioprinting technology, the Chinese experience could be interesting, since the PRC legislation differentiates legal regulation of relations in product liability and in liability for medical malpractice.

As noted in the scientific literature, the PRC Tort Liability Law 2010 provides for three models, by which a medical organization could be held liable: guilty model, guilt liability model with presumptive guilt and strict (non-fault) liability model[42].

The most acceptable standard of liability is established in regard to medical organization activities related to the patient diagnostics and treatment (Art. 54 TTL). It is of interest that Chinese lawmaker, as grounds for exempting medical organization from liability, indicated inappropriate behavior of the patient (his close relative), who avoids cooperation with the medical institution in accordance with relevant procedures and standards, as well as complexity of treatment and diagnosis, taking into account the current level of medicine (Art. 60 TTL).

Medical organization fault is presumed in case of violating information obligations; for example, medical risks and alternative medical treatment plans were not explained to the patient; patient's written consent was not obtained (Art. 55 TTL); if a medical professional did not fulfill diagnostic and treatment responsibilities in accordance with the established standard (Art. 57 TTL).

If the patient was harmed due to any defective medical product, medical instrument or

[40] Johnson v. Sears, Roebuck & Co., 355 F. Supp. 1065 (E.D. Wis. 1973).
[41] E. Lindenfeld, n 10 above, 79-103.
[42] L. Xiang and J. Jigang, *Concise Chinese Torts Law* (Springer 2014), 96-97.

transfusion of low-quality blood, the patient is entitled to demand compensation from manufacturer or institution that provided the blood, or demand compensation from the medical institution (Art. 59 TTL). In such circumstances, liability is imposed according to the strict (non-fault) standard, a characteristic feature of product liability.

Thus, legislation of the PRC, when elaborating the medical organization model liability, took into account the generally useful nature of medical activity connected to saving lives and health of people, as well as the legal nature of emerging relationship. Since medical services are often of experimental character, certainty or guaranteed result is missing, when they are provided, because it depends on many factors, including those not controlled by medical personnel. Therefore, as a basis for exemption from liability, it is indicated that difficulties in the patient diagnostics and treatment could be conditioned by the general level of medicine at the moment.

Considering the general level of medicine, as the basis for exemption from liability, recalls the rule provided for in Article 7 (e) of the Product Liability Directive 85/374/EEC that, manufacturer in order to be exempted from liability could prove that the state of scientific and technical knowledge during introduction of goods in circulation did not allow to identify this defect in the product (Development Risk Defense). Scientific literature notes that the purpose of this clause is to balance the interests of consumers in obtaining compensation for harm and the interests of manufacturers in relation to the possibility of innovative development[43].

This logic could be extended to liability for harm caused to the patient in using the bioprinting technologies. The following factors indicate the need to establish a guilt liability standard: 1) positive result is not guaranteed to a patient in case of transplanting a bioprinted organ, since the result depends on factors not controlled by a medical organization; 2) experimental nature of the bioprinting technology; 3) socially beneficial effect of technology capable of saving many lives.

3. Prognostic view of the model of liability for harm caused to the patient by the use of bioprinting technologies.

The question remains open, whether strict differentiation of the medical organization liability model is required depending on the type of its activity, i.e. technical (computer-aided) preparation to bioprinting and proper medical activity associated with patient treatment through the bioprinted organ transplantation. Is strict (non-fault) liability necessary for harm caused by a defect in the bioprinted organ computer-aided design, i.e. in the "computer-aided replica" content of a bioprinted organ (CAD files)?

It appears that such an artificial division of stages in bioprinting in order to elaborate separate liability models is inappropriate. Bioprinting is not just kind of mass production of medical devices, this technology would always be aimed at bioprinting a unique human organ for a particular patient taking into account individual characteristics of his organism. In our opinion, scientific position of Jamil Ammar, according to which it is necessary to differentiate liability of a medical organization in bioprinting by setting the liability non-fault standard for harm associated with drawbacks in computer-aided design when creating a computer-aided replica of a bioprinted organ (CAD files)[44] is controversial. The indicated author used the approach developed by other authors for the purpose of establishing a model of liability for harm caused by defects in designing the computer-aided models (CAD files) of medical

[43] L. Sterrett, 'Product Liability: Advancements in European Union Product Liability Law and a Comparison between the EU and U.S. Regime', 23 (3) Michigan State International Law Review, 885-925 (2015).
[44] J. Ammar, n 14 above, 37-67.

devices[45].

However, computer-aided design of medical devices manufactured using additive technologies based on inanimate nature materials, for example, of an individual joint endoprosthesis made of titanium and polymers, or a dental mouthguard made of thermophilic plastic, is not similar in complexity to computer-aided modeling of human heart, liver or kidney. Despite the fact that each dental mouthguard is being printed using thermophilic plastic based on a computer-aided model designed taking into consideration individual characteristics of a particular patient teeth and jaw structure, this is still massive, relatively simple and stream-fed technology.

Therefore, approach proposed by a number of authors setting the liability non-fault standard for harm caused as a result of drawbacks in computer-aided design and defectiveness of computer-aided models (CAD files) is justified in the 3D printing of medical devices, but is not applicable in bioprinting of human organs.

Bioprinting is a new, breakthrough technology that could save millions of lives. This technology is more complex compared to three-dimensional printing of medical products made from inanimate nature materials. In our opinion, if harm to the patient's health was caused by the presence of defects in the computer-aided model of a bioprinted organ, presumptive guilt model, which could be refuted by a tortfeasor, should be used. This model of guilt liability is basic for the Russian civil law, because according to Clause 2 of Article 1064 of the Civil Code of the Russian Federation, the person, who caused harm, is exempted from compensation for harm, if he proves that harm was caused not through his fault. The law may also provide for compensation for harm even, if the fault in causing harm is missing.

Thus, general rule in the Russian law is a model of tort liability with presumptive guilt, in which the burden of proving innocence rests with the person, who caused the harm. Guilt of causing harm is always assumed until proved otherwise. This distinguishes Russian law from the German law, since guilt in the Civil Code of Germany is presumed only in contractual, but not in the tort liability.

It should be noted that one of the main arguments provided by Jamil Ammar in favor of the liability strict non-fault standard for harm caused by defects in computer-aided design of a bioprinted organ model was a difficulty in proving the negligence (guilt) of the tortfeasor[46]. This argument is determined by specifics of the Anglo-Saxon tort law, in particular, by its basic tort based on guilt (negligence) of the tortfeasor (tort in negligence). To be held liable for such a tort, it is necessary to establish the tortfeasor duty to take care of the damaged physically person (duty of care), violation of such a duty, existence of harm and causal relationship between harm and duty violation[47]. However, these arguments are not working, if the liability model used is based on the tortfeasor presumed guilt.

In the prognostic aspect and in elaborating a fair model of liability for harm caused to a patient in connection with the use of bioprinting technologies, court position is of interest, which was expressed in judgement in the Wilkes v DePuy International Ltd case[48]; English literature pays serious attention to it[49].

In this case, the damaged physically patient was subjected to surgery to replace the hip joint. Artificial joint (implant) was manufactured by the defendant. Three years after the joint

---

45 E. Lindenfeld, n 10 above, 79-103. See also: E. Lindenfeld and J. Tran, 'Strict Liability and 3D-Printed Medical Devices', 17 Yale Journal of Law and Technology Online, (2015) available at SSRN: https://ssrn.com/abstract=2697245 (last visited 10 June 2020)

46 J. Ammar, n 14 above, 37-67.

47 D. Nolan, 'Deconstructing the Duty of Care',129 Law Quarterly Review 559-588 (2013).

48 Wilkes v DePuy International Limited [2016] EWHC 3096 (QB)

49 D. Nolan, 'Strict Product Liability for Design Defects', 134 Law Quarterly Review, 176-181 (2018).

replacement operation, the implant structural element broke due to "material fatigue". On this basis, the patient filed a lawsuit grounded both on the defendant tort in negligence and on the statutory rules of the Consumer Protection Act 1987 establishing strict (non-fault) liability standard. The judge in this case indicated that security is a relative category. Since, no product was absolutely safe; therefore, determination of the safety acceptable level was carried out taking into consideration the risk-benefit analysis. The court took into account that there was no evidence of a production defect in the implant and rejected the plaintiff's arguments that simple structural solutions could eliminate the risk of the implant early failure, since the alternative design proposed by the plaintiff had itself drawbacks, and the implant would become less convenient and more expensive. The damaged physically person was informed about the risk of the prosthesis destruction, as well as about dangerous factors increasing the risk level. The court pointed out that when assigning liability, it should be borne in mind that such consequences could be eliminated through the implant replacement operation and noted that it was necessary to take into consideration potential benefits for a particular patient from the use of medical goods and the risks that appeared with this patient.

However, Donal Nolan criticized position of the court and stressed that it was necessary to take into account benefits and risks not only for the individual patient, but also the "global" benefits, as well as those risks that generally arise, when using these products[50].

Thus, it is proposed to take into consideration not only the risks posed by certain products and technologies, but also their benefits on the general social scale, as well as the fact that in order to obtain any beneficial effect, the patient could voluntarily assume those risks that arise, when using one or another product or technology in the course of treatment.

Australian authors also point out from this position and indicate voluntariness in accepting the risk of harm by the damaged physically person as the basis for exempting the tortfeasor of liability for harm caused by using additive technologies. Such voluntary risk acceptance is only possible, if the damaged physically person was provided with full understanding of the existing risks, and he directly or indirectly expressed the waiver of his right for protection in case of harm[51].

In relation to the Russian law, rule of Paragraph 3 of Article 1064 of the Civil Code of Russia could be pointed out, according to which compensation for harm may be refused, if the harm was caused at the request of or with consent of the damaged physically person, and actions of the harm tortfeasor were not violating the moral principles of society.

4. Concluding remarks and future perspectives.

It looks like this norm would probably be of significant importance in resolving issues of liability for harm caused to a patient in connection to using the bioprinting technologies in treatment. Since the fact the patient is giving his voluntary informed consent to treatment using the bioprinting technologies could be qualified as taking by a patient the risk of possible adverse consequences beyond the medical organization control, for example, rejection of the bioprinted organ by the patient's organism. Such consent could be qualified as a circumstance that eliminates unlawfulness of causing harm and creates the basis for exempting a medical organization from liability for harm caused to the patient when using the bioprinting technologies.

[50] D. Nolan, n 38 above, 176-181.
[51] J. Nielsen and L. Griggs, n 24 above, 712-739.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

The use of it tools and artificial intelligence in the health sector: the patient as a vulnerable subject

FABRIZIA ROSA
Ph.D. Candidate at University Parthenope of Naples

Abstract

The present work aims at analyzing the development of technologies in the healthcare sector and the impact this has had on patients' right to privacy.

After having examined the meaning of "digital health", it focuses on the main tools used nowadays for the processing of patients' data (telemedicine, electronic medical records and electronic health records) and on the risks they entail for the protection of patients' right to privacy.

Notably, since the processing of data includes personal and health data stored digitally, these are exposed to the possibility to be lost or become inaccessible, violated or stolen, circumstances that can lead to problems both on the individual level regarding privacy violation, and at the collective level, for example impeding the provision of health services.

In conclusion, in order to minimize these risks it is necessary that digitalization in the health sector become an organic and safe process and that health data management strategies are envisaged to ensure the protection and availability of data in a reliable and timely manner.

Keywords: health - patient - technologies - privacy.

Summary: 1. The patient and his rights: in particular, the right to privacy and the processing of health data. – 2. The processing of patient data in the emergency context by Covid-19. – 3. The development of healthcare technologies: some examples of digital healthcare. – 4. Digital healthcare at the time of Covid-19. In particular, the innovations introduced with reference to the *Fascicolo Sanitario Elettronico* (FSE or Electronic Health Records). – 5. The benefits and risks of digital health. In particular, the impact of new technologies on the processing of health data. – 6. The challenges that digital health poses and the perspectives *de iure condendo*.

1. The patient and his rights: in particular, the right to privacy and the processing of health data. Brief reference to the implications in the current emergency context.

The health care relationship that is established between the healthcare facility and the patient includes a complexity and heterogeneity of services that cannot be easily determined in advance. In particular, it is characterized by considerable accessory services and organizational duties of the structure, with the consequence that it would not be sufficient to speak only of a medical-surgical service in the strict sense, but, at most, of an atypical *ad hoc* contract. For this reason, doctrine[1] and jurisprudence[2] have coined the atypical contract

[1] P Stanzone, V Zambrano, *Attività sanitaria e responsabilità civile* (Giuffrè, 1998), 505 ff.; M Toscano, 'Il difetto di organizzazione: una nuova ipotesi di responsabilità? (note to Court of Monza June 7 1995)' (1996) Resp. civ. e prev., 389 ff.

[2] In this sense, after several pronouncements from the jurisprudence of merit, the United Sections of Court of Cassation of 2002 were expressed, according to which '*The complex and atypical relationship that is established between the clinic and the patient (in this case: a pregnant woman), even if the latter chooses a treating doctor from outside the health care*

of expediency, to which the ordinary rules on non-performance established by art. 1218 apply. In particular, this term is intended to indicate the complex synallagmatic contract with corresponding services between the health facility and the patient, which includes - at the expense of the former - a whole series of services, additional to medical and / or surgical assistance, which consist, among others, in duties of management of medical and paramedical personnel, maintenance of machinery and premises of the structure, guarantee of maintenance of sanitary conditions necessary for the use of services, supervision and control of instruments and pharmaceutical products used and so on.[3]

Faced with all the above mentioned duties of the hospital, there are a series of rights due to the patient as such, to know about which it is essential to keep in mind the European Charter of Patients' Rights issued in 2002, which is a key reference point for all health care professionals, as well as for patients.

In particular, these include the right to information (the patient has the right to know all information regarding his or her state of health, the health services that can be used and how to access them); the right to consent (the patient has the right to know all useful information in order to be able to consent to the treatment he or she undergoes); the right to free choice (the patient, properly informed, has the right to choose freely between the various possible forms of treatment); the right to respect time limits (the patient has the right for each phase of treatment to receive treatment in a short and predetermined time); the right to respect quality standards (the patient has the right to high quality treatment); the right to safety (the patient has the right not to suffer damage from medical errors or malfunction of equipment and/or health services) and so on.

But the right we focus on here is the right to privacy: the citizen who comes into contact with health facilities for diagnosis, treatment, medical services, administrative operations and other, must be guaranteed the most absolute confidentiality and the widest respect of his or her fundamental rights and dignity.

As is well known, privacy is a set of rules created to ensure that the processing of personal data is carried out with respect for the fundamental rights and freedoms of everyone.

In the health sector, however, given the delicacy of the data processed and the position of the parties involved, the processing of personal data receives a specific discipline.

Before the entry into force of EU Regulation 2016/679 (c.d. GDPR: General Data

---

facility, is not limited to the mere provision of services of a hospitality nature (provision of board and lodging), but consists in the provision of auxiliary medical and paramedical personnel and the provision of medicines and all necessary equipment, even in view of any complications', Court of Cassation, United Sections, 1 July 2002, n. 9556, in Giust. civ., (2003), 2196.

This decision has then been followed by other pronouncements of the simple sections: see, in such sense, Court of Cassation, 3rd Civil Section, 13 January 2005, n. 571, in *Danno e resp.* (2005), 5, 563, which states the following principle: "*The relationship that is established between patient and private nursing home (or hospital institution) has its source in an atypical contract with protective effects on the third party, from which, against the obligation to pay consideration (which can well be fulfilled by the patient, the insurer, the national health service or another body) arise at the expense of the nursing home (or institution), in addition to those of broadly hospitality nature, obligations to make available auxiliary medical personnel, paramedical staff and the provision of all necessary equipment, including in view of any complications or emergencies. It follows that the responsibility of the nursing home (or the institution) towards the patient has a contractual nature, and may result, pursuant to art. 1218 of the Italian Civil Code, in the non-fulfillment of the obligations directly in its charge, as well as, pursuant to art. 1228 of the Italian Civil Code, the non-fulfilment of the medical-professional service provided directly by the health care professional, as his necessary auxiliary, even in the absence of a subordinate employment relationship, however, since there is a connection between the service provided by him and his company organization, not noting, on the contrary, the fact that the health care professional is also "trusted" by the same patient, or in any case by the same one*"; Court of Cassation, 3rd Civil section, 26 January 2006, no. 1698, in Mass. Giur. it., (2006); Court of Cassation, 3rd Civil section, 13 April 2007, n. 8826, in Mass. Giur. it. (2007).

[3] It is on the basis of these duties that the minimum requirements that a health facility must meet have been articulated.

Protection Regulation)[4], with particular reference to the processing of health data, the former Privacy Code (Legislative Decree 196/2003) provided that the same could be processed only with the consent of the person concerned and after authorization from the Guarantor (art. 26, paragraph 1). In other words, the consent of the interested party was given a central role as a legitimate prerequisite and condition of lawfulness of the processing of personal data. Therefore, the rule was that the personal data could be processed only with the consent of the person concerned and exceptions were provided for (and justified) only by the extraordinary nature of certain situations.

However, there were a number of cases in which the processing of health data was allowed even without consent, without prejudice to the need for prior authorization from the Guarantor. In particular, reference was made to the case in which the processing of data was *necessary* to safeguard the life or safety of a *third party*. If, on the other hand, the same need arose with reference to the person concerned and he or she was unable to give consent due to physical impossibility, inability to act or inability to understand and want, it was provided that the same was "manifested by those who exercise legal power, or by a close relative, a family member, a cohabitant or, in their absence, by the manager of the facility where the person concerned resides".

Similarly, art. 82 of the Privacy Code took into account emergency situations, providing that the information and consent to the processing of personal data could intervene "without delay, after the performance [of medical services]", when there was one of the following hypotheses: a) physical impossibility, incapacibility of giving consent of the person concerned, when it is not possible to obtain consent from the persons indicated in letter b) of art. 26; b) serious, imminent and irreparable risk for the health or physical safety of the person concerned; c) medical performance that may be affected by the prior acquisition of consent, in terms of timeliness or effectiveness.

From the combined reading of these articles, it emerged that, in fact, in the codicistic system there were no cases in which the processing of health data for the purposes of treatment of the person concerned could disregard the granting of consent (prior or subsequent, directly from the person concerned or from a third party, but always present and necessary).

Moreover, the previous system did not provide for the hypothesis in which the interested party, while requesting a health service necessary for the protection of her life or physical safety, could refuse to give consent to the processing of her personal data. According to the Code, in such a case, the doctor should have refused to provide the service.

Another unforeseen hypothesis was the one in which, since one of the hypotheses referred to in art. 82 existed, the doctor had already performed the service without requesting consent and subsequently the person concerned had refused to grant it. Here, a doctor that intervened promptly to safeguard the safety of the person concerned would have risked being called to answer for having illegally processed the patient's personal data.

In conclusion, the previous regulatory system provided that the processing of health data could only take place with the consent of the person concerned, except in exceptional cases.

However, it soon became clear that consent was inadequate as a legal basis for the processing of health data.

In this regard, the GDPR (EU Regulation 2016/679) intervened, overcoming the previous approach and introducing a new one for the management of personal data processing in the health sector.

[4] EU Regulation 2016/679 came into force on May 24, 2016, but has been applied in EU States since May 25, 2018. In Italy, the GDPR was implemented by Legislative Decree no. 101/2018, which came into force on September 19, 2018.

With EU Regulation 679/2016, in fact, the centrality of consent has disappeared, in the sense that it is only one of the possible alternatives (or rather, legal bases) on which the processing of personal data can be founded, placing itself on the same level with respect to the other 5 legitimizing assumptions - all abstractly suitable to constitute a condition of lawfulness for the processing of data.

The lack of the centrality of consent is even more evident with reference to the processing of special categories of personal data, such as those "*related to health*", which, among other things, find for the first time in the GDPR their specific definition: they are "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*" (art. 4 GDPR).

In fact, unlike in the past, the health professional no longer has to request the patient's consent for treatment regarding essential services (clearly, this refers only to the treatment necessary to achieve the specific "treatment purposes" provided by the GDPR itself, and not also to those carried out for different purposes, such as promotional, commercial and so on).

But let's go in order.

The new configuration of the Regulation is based on the combined provisions of art. 6 and art. 9 dedicated to the "*Processing of special categories of personal data*".

First of all, since "health-related data" are included among the special categories of personal data, which, by their nature, are particularly sensitive and, therefore, need a higher level of protection, they are subject to the general prohibition of processing (art. 9, par. 1); secondly, the prohibition, derogated from the following par. 2 which allows the processing of the same provided that at least one of the ten conditions listed therein is met. In particular, for the health sector, the conditions set forth in letters g), h) and i) are relevant[5].

Letter g) refers to the hypothesis of relevant public interest on the basis of EU law or Member States; letter h) refers to treatment purposes, i.e. preventive medicine, diagnosis, health or social care or therapy or management of health or social systems and services on the basis of EU or Member State law or in accordance with the contract with a health professional (see also par. 3 of the GDPR and recital no. 53); letter i) refers to hypothetical cases of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicinal products and medical devices, on the basis of Union or Member State law providing for appropriate and specific measures to protect the rights and freedoms of the person concerned, in particular professional secrecy (see also recital 54) (e.g. health emergencies following earthquakes and food safety).

Moreover, the possibility for national legislators to introduce stricter conditions, aimed at ensuring a higher level of protection than that resulting from the Regulation (art. 9, par. 4), remains unchanged.

In any case, from May 25, 2018 (date of definitive applicability of the GDPR), the existence of the assumptions provided by letters g), h) and i) will be sufficient conditions to allow the processing of the health data of patients, without the need to acquire their consent.

Once the existence of one (or more) of the above conditions has been ascertained, the general prohibition of processing as per paragraph 1 of art. 9 will be lifted, with the consequence that health data can be processed, similarly to the "ordinary" categories of personal data, referring to one of the legal bases as per art. 6.

Art. 6, in fact, in regulating the lawfulness of the processing, lists six different legal bases among which the data controller, consistently with the principle of accountability, must identify the most appropriate one at any given moment. In this list, the consent of the person

[5] In this regard, see Gruppo di lavoro Bioetica COVID-19, 'Protezione dei dati personali nell'emergenza Covid-19', Rapporto ISS COVID-19 No. 42/2020 (2020), version of May 28, 3.

concerned appears only as one of the possible alternatives on which the processing of personal data can be based and is on the same level as the other legitimate assumptions.

However, since, as previously stated, consent cannot constitute a valid legal basis for the processing of personal data necessary for the provision of health services (since, to repeat, failure to do so would make it impossible to receive the requested service), a different legal basis must be identified.

The second step, therefore, consists in identifying the most appropriate legal basis for such processing, which once identified, will make it possible to process data relating to health.

Therefore, there is no longer a relationship as a rule - exception, but rather a plurality of equal conditions are identified.

In fact, the doctrine[6] is now in agreement in affirming that the Regulation has equalized the consent of the interested party to any other legitimate basis provided by law: "*These are conditions that are equivalent to each other and equal in order, it being sufficient that there is at least one that is able to consider the first stage of the evaluation process as regards the lawfulness of the processing to be passed*"[7].

Once the approach outlined by the GDPR has been defined, it is appropriate to consider how this is coordinated with the Italian regulatory system.

In Italy, on 19 September 2018, Legislative Decree no. 101 of 10 August 2018, containing provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 (so-called adaptation decree), came into force.

This decree confirmed the approach of the Regulation with reference to both the six legal bases of the processing and the ten conditions for the processing of special categories of personal data, thus confirming the possibility of processing data relating to health even without the consent of the person concerned. Of particular importance was the repeal of art. 81 concerning the "*Provision of consent*", which provided for the possibility to express orally the consent to the processing of data suitable to reveal the state of health, with annotation of the health professional for the purpose of documenting the granting of consent. This abrogation, in a rather clear-cut way, confirms the disappearance of the need to acquire the patient's consent and, among others, demonstrates the legislator's intentions to fully adapt the national regulations to the Regulation, overcoming, also with reference to health data, the previous concept based on the centrality of consent.

In any case, regardless of the decree of adaptation, as of May 25, 2018 the Regulation is definitively applicable in all Member States, with automatic disapplication of all national rules incompatible with it.

Consequently, from that date, even in the absence of the adjustment decree, it has become possible to process health-related data for medical purposes without the need to obtain the consent of the person concerned, provided that one of the conditions set forth in paragraph 2 of Art. 9 of the GDPR is met and the processing is based on one of the legal bases set forth in paragraph 1 of Art. 6 of the GDPR.

---

[6] See L Lipari, 'Privacy: dal Regolamento (UE) 2016/679 al d.lgs. n.101/2018' (2019), 7 February, diritto.it: '*the failure to give consent when data are processed for diagnosis and treatment (art. 2-septies of the Privacy Code amended by Legislative Decree no. 101/2018 in combination with art.9 GDPR)'* would represent the transition '*from a consensus-centric system to a system where it is necessary to first ask oneself and understand the reasons why the data are processed, and then evaluate, in light of the identified purpose, the basis of lawfulness of such processing'*. Available at https://www.diritto.it/privacy-dal-regolamento-ue-2016-679-al-d-lgs-n-101-2018/. On this point, see also G Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Zanichelli 2017) 101 ff.; and L Bolognini - E Pelino – C Bistolfi, *Il Regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali* (Giuffrè 2016) 277 ff.

[7] G Finocchiaro, *Il nuovo Regolamento europeo sulla privacy,* (n 6) 126.

2. The processing of patient data in the emergency context by Covid-19.

The treatment of health data in the current emergency context of the Covid-19 pandemic merits a brief, but necessary, mention.

Given what has been said in the previous paragraph - that is, that art. 9 par. 2 GDPR lists the exceptions to the general prohibition of processing "special categories of data", including those on health, making them lawful to process, in particular when of interest to letters g), h), i) - it must, first of all, be emphasized that in a situation such as the one in which we, unfortunately, still find ourselves, the data processing activity falls within the hypothesis provided by art. 9 par. 2 letter i) of the GDPR which, to reiterate, allows the processing of health data when it "is necessary for reasons of public interest in the public health sector".

It is no coincidence that decree-law no. 14 of March 9, 2020, containing urgent provisions for the strengthening of the National Health Service in relation to the emergency of COVID-19 (published in Gazzetta Ufficiale no. 62, on March 9, 2020, and in force from March 10, 2020) allows a simplified regulation for the protection of personal data based, in fact, on art. 9 par. 2 letter i) of the Regulation[8].

In particular, the aforementioned Legislative Decree no. 14/2020, emphasizes that the simplified rules for the protection of personal data in the health emergency - which are temporary in the sense that they are intended to have a duration no longer than the duration of the state of emergency - are designed to make the exchange of information between health authorities easier and faster, as well as speed up and streamline the process of clinical trials of new medicines, protocols and medical devices; in addition, the increase in the archiving potential of patient information makes the entire system of management of the current health crisis more fluid and effective.[9]

Also of interest, we should highlight the need, emergent from the current emergency context, to properly manage personal data related to health that may be useful for scientific research and statistical data collection.

Given the sensitivity of the issue and the data processed, on April 21, the EDPB (European Data Protection Board) intervened on the issue by adopting specific "Guidelines" on the processing of health data for scientific research purposes in the context of the Covid-19 emergency, aimed at addressing the fundamental legal aspects of the case. The EDPB clarifies that the GDPR already contains numerous provisions on the processing of health data for scientific research purposes, which also apply in the context of the pandemic[10]. In addition, the document recalls that it is still necessary to respect the principles provided by Article 5 of the GDPR, including, in more detail: transparency; purpose limitation; data minimization and storage limits; integrity and confidentiality.

Subsequently, at the national level, the Guarantor for the Protection of Personal Data intervened on this point and, having examined the EDPB "Guidelines", dedicated a section of the FAQ on Covid-19 to "Data processing in the context of clinical trials and medical research in the context of the Covid-19 health emergency".

In particular, the legal bases that are indicated necessary so that, in the current emergency context, the processing of this particular category of personal data may be considered lawful are (alternatively): (i) the consent of the patient (art. 9 par. 2 letter a); (ii) the reasons of relevant public interest (art. 9, par. 2, letter g) GDPR); reasons of public interest in the field of public health (art. 9, par. 2. letter i); purposes of archiving in the public interest, scientific or historical research or statistical purposes in accordance with article 89, paragraph 1 (art. 9

[8] See Gruppo di lavoro Bioetica COVID-19, "*Protezione dei dati personali nell'emergenza Covid-19*", (n 5), 8.
[9] G Resta, 'La protezione dei dati personali nel diritto dell'emergenza Covid-19' (2020), 5 May, Giustiziacivile.it,.
[10] For example art. 5, par. 1, lett. b) and lett. e); art. 14, par. 5, lett. b); and art. 17, par. 3, lett. d) GDPR.

par. 2 letter j).

The National Guarantor for the Protection of Personal Data in its analysis also pointed out that the issue of processing necessary for reasons of relevant public interest (Article 9, paragraph 2, letter g) GDPR) could have created difficulties at this specific time and, therefore, deemed it necessary to introduce exceptions.

This is because it is precisely the public interest and public health that, in this particular period of health emergency, risk being in conflict with the interests and the right to the protection of personal data of patients affected by COVID-19, who witness the use of their data for the diagnosis and treatment of the disease, for scientific research and for statistical purposes. Therefore, the need to balance the interest of the protection of personal data and the interest of the protection of public security (*rectius*, health) emerges in all its scope.

Creating difficulties in this balance were in particular the provisions of art. 110 of the Privacy Code (Legislative Decree no. 196/2003 amended by Legislative Decree no. 101/2018), which contain the actual content of art. 9 par. 2 letter j) GDPR in conjunction with art. 6 par. 1 letter. f) providing that "*The consent of the interested party for the processing of data relating to health, for the purposes of scientific research in the medical, biomedical or epidemiological field, is not necessary when the research is carried out in accordance with provisions of law or regulation or European Union law in accordance with Article 9, paragraph 2, letter j) of the Regulation, including the case where the research is part of a biomedical or health research program provided under Article 12-bis of Legislative Decree no. 30 December 1992. 502, and an impact assessment is conducted and made public pursuant to articles 35 and 36 of the Regulation*".

Art. 110 continues with "*consent is also not necessary when, due to particular reasons, informing the interested parties is impossible or involves a disproportionate effort, or is likely to make it impossible or seriously jeopardize the achievement of the objectives of the research. In such cases, the data controller adopts appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, the research program is subject to a reasoned favourable opinion of the competent ethics committee at territorial level and must be submitted for prior consultation with the Guarantor*".

These provisions and requirements would have risked blocking the collection of data to carry out the research necessary to counter the epidemiological crisis of COVID-19 and, such blocking, could clearly not be permitted to occur. Hence the decision to intervene with FAQ, introducing a derogation, albeit partial, to art. 110 in cases of data processing concerning experimental studies and compassionate uses of medicinal products for human use for the treatment and prevention of the virus, establishing that "*holders who intend to carry out processing of personal data relating exclusively to experimental studies and compassionate uses of medicinal products for human use, for the treatment and prevention of the Covid-19 virus, are not obliged, under the legislation relating to this emergency phase, to prior submission of the research project, or of the related impact assessment or to submit the prior consultation of the Guarantor referred to in art. 110 of the Privacy Code*".

Therefore, despite the fact that European and national legislation on the processing of personal data applies also in this particular emergency phase, the need has emerged to adapt this legislation to the necessity to collect data from patients affected by COVID-19 for scientific research purposes, in order to find the medicines and treatments suitable for the treatment of this new virus, striking a balance between the rights of the patient concerned, which are partially limited, and the public interest in health protection[11].

From what has been said so far - given the close connection between personal confidentiality and public safety - the need to give priority to collective safety (and health) over the protection of individual health data has clearly emerged.

In the face of this, however, it must be stressed that, if it is true that in emergency

[11] V Lemma, 'COVID-19: il trattamento dei dati sanitari tra privacy e interesse pubblico' (2020), 8 June, osservatoriomalattie.rare.it.

situations the right to the protection of personal data must be balanced with higher-ranking rights (such as the right to safety and public security), this does not mean that the same can be arbitrarily compromised[12]. In fact, any of its limitations must respect the canons of reasonableness and proportionality[13] and cannot go so far as to affect the essential content of the law itself, since it can never (and must never) involve the integral sacrifice of the intangible core of the fundamental rights of the human person.

In this sense, finally, the jurisprudence of the European Courts has intervened, which has helped to define the impassable stakes and the minimum or essential content of the right to data protection, recalling the principles of proportionality and strict necessity of the limitations concretely adopted[14].

3. The development of technologies in the health sector: some examples of digital healthcare.

Having provided a premise about the meaning of "health data" and the processing of health data, we now move on to analyse what the impact of the development of technologies in the health sector has been and what problems have arisen, particularly with regard to the patient's right to privacy.

New technologies and, in particular, the digitization of information - with the possibility of its sharing and use granted by the Internet - have created new forms of cultural, professional and organizational interaction in the health sector and have had repercussions on the traditional way of managing health and illness, with respect to the doctor-patient relational approach and related medical-legal aspects.

With current technologies, examinations are faster, diagnoses more accurate and all information, images, reports and consultations can "travel" digitally. Thanks to an internet network capable of supporting high data flows, it is possible to monitor and manage patients through systems that allow ready access to their clinical profiles even remotely, a possible

---

[12] See in this regard F Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali* (Giappichelli, 2016) 21. See also B Caravita, 'L'Italia ai tempi del coronavirus: rileggendo la Costituzione italiana' (2020), 6, Federalismi.it; L Panzani, 'COVID-19. Un'emergenza destinata a protrarsi. Appunti per il "dopo"' (2020), 10, Federalismi.it; M Tresca, 'Le fonti dell'emergenza. L'immunità dell'ordinamento al covid-19' (2020), 3, Osservatorio AIC; E Grosso, 'Legalità ed effettività nel tempo del diritto costituzionale dell'emergenza' (2020), 16, Federalismi.it; M Cartabia, 'Nella Costituzione le vie per uscire dalla crisi. Possibili limitazioni ai diritti ma proporzionate e a tempo' (2020), 29 April, interview in Corriere della sera, 9. See also G Resta, 'La protezione dei dati personali nel diritto dell'emergenza Covid-19' (n 9), in which the author refers to the "*right to human intervention*" in art. 22 GDPR, to be taken "*as the north star of a fruitful interaction between man and machine, aimed at the simultaneous realization of two fundamental rights, that of health and that of the dignity of the person*".

[13] M Cartabia, 'Nella Costituzione le vie per uscire dalla crisi. Possibili limitazioni ai diritti ma proporzionate e a tempo' (2020), 29 April, interview on Corriere della sera, 9; M Cartabia, 'I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana', speech presented to: Incontro trilaterale tra la Corte costituzionale italiana, la Corte costituzionale spagnola e il Tribunale costituzionale portoghese, Rome, (2013); G Scaccia, Il principio di proporzionalità, in S Mangiameli (ed.), L'ordinamento europeo. L'esercizio delle competenze (vol. II, Giuffrè, 2006), 225-274.

[14] Judgment of 9 November 2010, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, joined cases C-92/09 e C-93/09, EU:C:2010:662; Judgment of 8 April 2004, Digital Rights Ireland and Kärntner Landesregierung, joined cases C- 203/12 e C-594/12, EU:C:2014:238; Judgment of 21 December 2016, Tele2 Sverige, C-203/15, EU:C:2016:970; Judgment on the merits delivered by a Chamber, *Antović e Mirković v. Montenegro*, no. 70838/13, § 42, ECHR 2017; Judgment on the merits delivereb by Grand Chamber, *Bărbulescu c. Romania,* no. 61496/08, ECHR 2017

prescription of medical care and the use of expert advice, regardless of where they reside.[15]

Therefore, not only the clinical-assistance processes, but also those concerning the management of patient data are subject to great changes.

The biggest and most recent innovation in the healthcare field concerns the use of information technology and is dubbed e-Health[16]. The term generally refers to any exchange of health data, collected and analyzed with the help of electronic and computer technologies, to improve the effectiveness and efficiency of health care[17]. To simplify, "e-Health" refers to the way in which information and communication-based technologies support health-related areas.

Among the various tasks assigned to digital health are: (i) care; (ii) surveillance; (iii) studies to promote prevention and diagnosis; (iv) treatment and monitoring of patient conditions and so on. And, in order to achieve these goals and for the results to be as expected the most cutting edge (and increasingly so) technology and artificial intelligence tools are used today.

It is evident that the rapid development of technology in the healthcare field has radically changed, in recent years, (and is still changing) the practice of medicine and its future developments.

In this regard, it cannot be underestimated that, further spurred by the COVID-19 health emergency, digital healthcare is making important steps forward.

In fact, physicians are increasingly connected with patients through digital channels and artificial intelligence is showing its potential for customization of care. In this respect, the pandemic has been an opportunity to experiment with solutions aimed at containing contagion, reducing hospitalizations and managing patients in a given locality; but also to redesign new models of care by accelerating the transition to a more connected, sustainable and resilient healthcare model.

From this point of view, it can be said that medicine and technology are evolving towards a connected healthcare model, the so-called Connected Care.

In order to fully understand the extent of the impact of the development of technologies in health care, it seems appropriate to focus on some of the most widespread tools used today: telemedicine, electronic medical records (CCE) and electronic health records (FSE in Italy - *Fascicolo Sanitario Elettronico*).

Among the most direct new developments in the digitization of healthcare, there is, first of all, ***telemedicine***. The term is a neologism resulting from the composition of two words: telematics (i.e. the set of applications derived from the integration of information technologies with those of telecommunications, based on the exchange of data or access to archives through the telephone network or special networks) and medicine. As is evident, telemedicine involves three different scientific-disciplinary areas: telecommunications, information technology and medicine.

This tool, in fact, involves the use of telecommunications, as well as electronic and information technologies to support medicine when the patient is geographically separate from the medical staff. Appropriately, therefore, telemedicine is defined as "the remote use of medical expertise in the place where the need arises"[18].

---

[15] M Zagra - S Zerbo - A Argo, 'Informatica, web e telemedicina', in M Zagra - A Argo – B Madea (ed.), *Problem-oriented forensic medicine* (Elsevier, 2011), 123 ff.

[16] '"eHealth" replaces the older term telemedicine', WHO, Building Foundations for eHealth, Report of the WHO Global Observatory on eHealth, 2006, 2.

[17] J P Harrison – A Lee, 'The Rule of E-Health in Exchanging Health Care Environment' (2006), 24(6), Nurs Econ., 284

[18] This definition can be found in Telemedicine Glossary, Glossary of standards, concepts, technologies and users. European Commission Information Society Directorate-General - Unit B1 Applications relating to Health edited by Dg Infso- B1 version 2.10, May 2000. The value of this definition consists in highlighting the

Even more comprehensive is the definition approved at the EU level, for which telemedicine is "the integration, monitoring and management of patients, as well as the education of patients and staff, using systems that allow ready access to expert advice and patient information, regardless of where the patient or information resides" (AIM 1990)[19].

It is a digital tool that simplifies and improves healthcare procedures between doctors and patients, especially in monitoring health conditions.

Telemedicine, therefore, represents an innovative approach that reorganizes the health care network between doctor and patient, facilitating the provision of services at a distance by using digital devices.

Prevention, diagnosis, treatment and patient monitoring can be performed even without going to traditional health care facilities, with the advantage of simplifying and making the best care accessible to all through a secure exchange of information, images and documents between professionals and patients.

In the current context of the Covid-19 health emergency, telemedicine has intervened (and still intervenes) to manage emergency activities in a timely manner, exploiting the immediacy of digital technology to exchange clinical information in the health network and improving the management of critical or unreachable patients.

This tool, however - like those that will be examined below - presents some critical aspects, such as the protection of the right to patient confidentiality, which should not be underestimated, and which we will address shortly.

Another important tool is the ***electronic health record (EHR***, also known by its most commonly used brand acronym, CCE, provided by the technology company IBM), which is the digital evolution of the traditional medical record, i.e. in paper format[20].

It represents, therefore, an instrument to support clinical decision-making processes, as it is the manager of the complete history of the patient, both inpatient and outpatient, promoting the continuity of the latter's care through the archiving of all clinical episodes related to the same hospital structure.

It is an essential starting point to have the information related to the patient's clinical history as soon as possible, in order to achieve an overall improvement in the quality of care[21].

In other words, it is a "virtual file that contains the clinical records and past, present and

---

evolution of the concept of telemedicine from a mere "practice of medicine without the usual physical confrontation between doctor and patient, using an interactive multimedia communication system" (BIRD, 1975) to the use of the same to overcome the problem of spatial distance between doctor and patient. For a general overview of the phenomenon of telemedicine, see E Coiera, *Guida all'informatica medica, Internet e telemedicina* (Il Pensiero Scientifico, 1997).

[19] This definition, in addition to highlighting, like the previous one, the evolution of telemedicine in the sense of solving the problem of the physician-patient spatial distance, also focuses on the Anglo-Saxon concept of "telehealth", which brings with it a revolution in the health system, in all its aspects, from medical organization to the management of emergency services and health education in general. In this regard, it seems enlightening the definition that, already back in 1976, the Committee for Telemedicine created by the University of Rome gave telemedicine, seeing it as "*a global system of reorganization of health structures in which modern means of telecommunications constitute the backbone*".

[20] On the definition of "medical record", see A Rossi - R. Maceratini, 'La cartella clinica elettronica (Electronic Patient Record)', in R Maceratini - F Ricci (ed.), *Il medico online - Manuale di informatica medica* (Verduci Editore, 2000), chap. VI. The guidelines of the Ministry of Health of June 17, 1992 ("The compilation, coding and management of the hospital discharge form established ex D.M. 28.12.1991"), define the medical record as "*the individual information tool designed to detect all significant personal and clinical information relating to a patient and a single episode of hospitalization".*

[21] G Cangelosi, 'I servizi pubblici sanitari: prospettive e problematiche della telemedicina' (2007) 1, Dir. fam. e pers., 440.

future information tied to the physical and mental health of the patient"[22].

At the international level, among the many existing definitions of "medical record", the most synthetic and effective one reads: *"The medical record is the who, what, why, when and how of patient care during hospitalization*"[23].

In conclusion, it is a digital document created by the healthcare facility that cares for the patient, which can also be shared with their family doctor and other specialists and which allows the complete dematerialization of the document production, with a management of information from a digitalized origin.

Finally, among the tools mentioned above, there is the ***electronic health record (FSE*** in Italy), which aims to provide health system operators with a global and unique vision of the health status of each citizen.

Established with Legislative Decree no. 179 of 2012, which defines it as "the set of digital data and documents of a health and sociomedical type generated by clinical events present and past, concerning the patient"[24], it represents the tool in which to bring together information and clinical documents of individual citizens generated in various ways by the national health service (SSN in Italy). It contains health events and documents summarized and organized according to a hierarchical structure, which allows to navigate through the documents in alternative ways depending on the type of investigation to be carried out.

Its introduction, in addition to streamlining the time-consuming processes dictated by the paper-based management of patient clinical information, leads to an improvement in the quality of services and significant cost containment.

Therefore, the FSE - unlike the electronic medical records, managed by the individual hospital - has the citizen as its center and was created to respond to the need for sharing clinical data and the principle of "interoperability" (on which, we will focus shortly).

4. Digital healthcare at the time of Covid-19. In particular, the innovations introduced with reference to the Electronic Health Record (FSE).

The usefulness and effectiveness of digital health tools (all, not only the FSE), where correctly and uniformly used, has emerged, in all its scope, in the current health emergency situation caused by Covid-19, which has highlighted two aspects: (i) the need to innovate and adapt these instruments to the current context and, therefore, to this situation's new needs, trying to ensure their linear and homogeneous use throughout the national territory; (ii) the need, increasingly felt, to find a solution to the risks that could arise from a distorted use of these digital health instruments, with particular attention to the protection of the patient's right to privacy.

With regard to the first aspect, it seems appropriate to dwell, in particular, on the relaunch of the Electronic Health Record (FSE), on whose discipline the Government wanted to propose important reforms in light of the recent experience gained in the pandemic by COVID-19.

Indeed, this instrument should have been activated in all regions and autonomous provinces by June 30, 2015, but, at the beginning of the pandemic, it was used in very few

---

[22] C Rabbito, 'La cartella clinica elettronica ed i suoi vincoli giuridici' (2007), June, Telemeditalia – Giornale di tecnologia medica, rubrica telesalute. The article highlights how the design of an eHealth system, which provides for the computerization of medical records, must necessarily take into account the particular nature of "public act" of the so-called "virtual file" and the consequent responsibilities (including criminal) of the various officials who will intervene on it in the insertion, modification and storage of health information.

[23]Source: American Hospital Medical Record Association

[24] Art. 12 of Legislative Decree no. 179 of October 18, 2012, on "*Further urgent measures for the growth of the country*" (converted, with modifications, from l. 17 December 2012, n. 221).

Italian regions and activated only by 20% of the population[25].

Therefore, in order to facilitate its use and encourage its activation, the legislator intervened by amending Article 12 of Legislative Decree No. 179 of 2012, through Article 11 "*Urgent measures on FSE*" of Decree-Law No. 34 of May 19, 2020 (the so-called "Relaunch" Decree), in particular, expanding the types of health data that must be fed into the FSE - making explicit reference to all digital health and sociomedical documents, referring to the services provided both by the National Health Service (SSN - *Servizio Sanitario Nazionale*) and outside the SSN - and, above all, widening the number of subjects qualified to feed the FSE, including, in addition to the patient with the medical data in their possession, also the health care professionals who take care of the patient both within the SSN and regional social and health services, and outside them. Therefore, there is also an opening of the FSE to private subjects whose systems will have to interact with the public standard and comply with the defined safety measures[26].

In addition, the decree eliminates the requirement of consent (free and informed) of the person concerned-assisted to the FSE (repeal of paragraph 3-bis of Art. 12 of Legislative Decree no. 179 of 2012); however, consent remains a condition *sine qua non* of the activation and consultation of its file.

The above changes made to the FSE offer many a food for thought.

In particular, as far as of interest here, there is to be considered that if, on the one hand, all these interventions lead to an increase in the use of the FSE, on the other hand one cannot but wonder if - in the face of an increase in data flows and subjects who will interact with the different FSE systems - the certainty of the origin and correctness of the data themselves can be fully guaranteed, as well as the accessibility of the same only by legitimate subjects[27].

And in fact, given that the task of making access to FSE information operational is the responsibility of the Regions - which must also promote interoperability throughout the national territory through the technical specifications published by the AgID (Agency for Digital Italy)[28] - cannot underestimate the fact that, to date, digital health is evolving discontinuously with respect to the different regional plans[29], and this does not always allow to meet the needs of interoperability and security[30].

Let's explain further. In the light of what is prescribed by the GDPR, the archiving system of documents present in the FSE is subject to the preparation of technical-organizational models and security measures aimed at ensuring the application of the European Regulation[31]

---

[25] See in this regard the monitoring activities divided into two distinct groups of indicators: Implementation and Use, available on the Agid website at the following link: https://www.fascicolosanitario.gov.it/monitoraggi.

[26] See Gruppo di lavoro Bioetica COVID-19, 'Protezione dei dati personali nell'emergenza Covid-19' (n 5), 15.

[27] A Fiaschi, 'Fascicolo Sanitario Elettronico: i rischi per la data protection delle politiche di sanità integrata' (2020), 28 January, *Cybersecurity.it.*

[28] For the specifications you can consult the following link: https://www.fascicolosanitario.gov.it/sites/default/files/docs-pdf/Specifiche-tecniche-per-l-interoperabilit-tra-i-sistemi-regionali-di-FSE-Framework-e-dataset-dei-servizi-base.pdf.

[29] G Pellicanò, 'Sanità digitale, stato dell'arte e prospettive future' (2019) 14, Smart eLab, available at the following link: https://calliope.cnr.it/index.php/smartelab/article/view/79/85.

[30] E Sorrentino, AF Spagnuolo, 'La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico' (2020), 30, federalismi.it, 252.

[31] Before 2016, the year in which the GDPR comes into force, the regulatory references for safety measures were those which can be found in the Personal Data Protection Code, Annex B and the guidelines. In particular, the Guidelines on online reporting (Chapter 6) highlight how: "*The particular sensitivity of personal data processed through online reporting services requires the adoption of specific technical measures to ensure appropriate levels of security pursuant to art. 31 of the Code, without prejudice to the minimum measures that each data controller must in any case adopt pursuant to the Code (art. 33 et seq.) and, in particular, where applicable, those required by rule 24 of the Technical Specifications on minimum security measures, Annex B) to the Code*".

and designed to avoid the risks arising from the destruction, loss, modification, unauthorized disclosure or access, accidentally or illegally, of personal data transmitted, stored or otherwise processed[32].

Therefore, following the lines of the legislator, the system should , in addition to confidentiality, integrity and availability of data, also ensure the security of the same through the adoption of all measures required by the legislation on privacy and by specific measures taken by the Guarantor of the health sector[33].

However, as mentioned above, the data under examination - which, through the FSE, are aggregated virtually and made visible - cannot always count on adequate resources to ensure uniform security measures.

And, therefore, if it is true that, as a result of the above mentioned changes, an attempt is being made to enhance the use of the FSE, it is equally true that it is underestimated that not all the producers called to feed the various FSE use document management and storage systems aligned with the regulations and such as to ensure adequate levels of security and privacy required by the GDPR.

In short, if in theory the FSE tool seems to overcome all the problems existing in the field of electronic medical records (in particular, those concerning the limitations imposed by privacy regulations and the impossibility, even with the patient's consent, to directly transfer the data of the CCE of one hospital to another), in practice, one has to deal with the risks involved, including the risk that during the input phase[34] (for which, please note, the consent of the person concerned is not required), potentially vulnerable data and documents are made available on the FSE, if there is no proper management of the entire life cycle of the document upstream.

In this regard, it can certainly be stated (anticipating what will be said in the last paragraph) that the interoperability of health data - understood as the ability of several systems to exchange information between them and to be able to use them - can be considered the first challenge to ensure that the opportunities of digital health do not remain only as such but are transformed into something concrete.

For the transfer of data suitable for revealing the genetic identity of an individual, the "*Linee guida in tema di Fascicolo sanitario elettronico e di dossier sanitario"* (Chapter 10) highlight that: "*The particular sensitivity of personal data processed through the FSE/dossier requires the adoption of specific technical measures to ensure appropriate levels of security (art. 31 of the Code)*". The principle of accountability or responsibility, introduced by the European Regulation, requires the preparation of adequate policies on data protection and, therefore, are no longer considered sufficient minimum security measures. In other words, today the Data Controller must adopt technical and organizational measures, including certified ones, that are concrete and always demonstrable, as well as Compliance with these Regulations. By virtue of the principle of privacy by design, it is also necessary that all of the required devices are used from the design phase of the system architecture. In this regard, see the 'Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali' (and in particular the Risk Based Approach and accountability measures (accountability) of Owners and managers).

[32] Opinion on the 'Linee Guida sulla formazione, gestione e conservazione dei documenti informatici' of February 13, 2020 available at the link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283921. The Guarantor clarifies, among other things, that the security measures referred to by the GDPR, in fact, replace the minimum ICT security measures for public administrations set out in the Guidelines issued by AgID in 2017.

[33] E Sorrentino, AF Spagnuolo, 'La sanità digitale in emergenza Covid-19' (n 28).

[34] The ESF is not fed homogeneously, which is a consequence of different interpretations and implementations by the Regions and Autonomous Provinces, both in reference to the use of document formats and in relation to the set of metadata to be associated with the documents. See in this regard by E Sorrentino and others, 'La conservazione dei documenti che alimentano il Fascicolo Sanitario Elettronico' (2020) 2(1), Riv. ita di informatica e diritto, 38.

5. The benefits and risks of digital health. In particular, the impact of new technologies on the processing of health data.

Even before the current health emergency, but now all the more so, the pervasiveness of information technologies within the healthcare world has fueled a process of profound renewal based on data.

In addition, the significant expansion of telemedicine solutions and the emergence of innovative solutions have led to informed patient participation and increased their personal well-being.

In fact, thanks to new technologies and the Internet, patients are more informed than ever before about medical conditions and treatments and play an increasingly active role in their care pathways.

One of the main advantages of digital healthcare is the possibility to guarantee complete interconnection, no longer linked to the location of a facility or the times when it is possible to book a medical examination.

This aspect has come to light, as never before, during this pandemic, which has shown how digital technologies - for example, electronic prescription and telemedicine - can allow the continuation of treatment even in a social distancing regime.

From this point of view, the increase of the general interest of health systems to speed up the digitization process is more and more evident; in this way, on the one hand, the reduction of the actual costs of treatment is obtained and, on the other hand, at the same time, a greater accuracy of diagnosis and procedures is guaranteed.

In this process of renewal, modern medical technology has therefore become dependent on the ability to collect and store patient data, image files, videos and a wide range of documents of various types. The inevitable result is the creation of large volumes of data that continue to grow at an increasingly rapid pace, largely unstructured, managed by a variety of different applications and systems and accessible by healthcare facilities, specialists and researchers.

But while it is true that the electronic storage and management of patient data offers substantial clinical and operational benefits, it also introduces new risks.

In particular, although of interest, it should be considered that a technology that is not well governed can cause problems both on an individual and collective level.

On an individual level, if patient data are lost or become inaccessible due to natural disasters or deliberate actions affecting the systems that host them, the consequences can be very serious: think, for example, of the lack of information about a patient's severe allergy to certain drugs.

In addition, knowledge of such "sensitive" data as genetic or health data, can lead to discrimination (think of the employment or insurance relationship) or in any case very relevant prejudices for the person concerned and violate, sometimes irreversibly, that right to the intangibility of one's private life which is the oldest root of privacy.

On a collective level, it must be considered that digitally stored data can also be violated or stolen, exposing patients' medical, personal and financial information and leaving operators vulnerable to ransomware attempts.

Attacks on healthcare information systems - a significant part of *cyber attacks* in our country - can have devastating effects on all citizens, preventing the delivery of healthcare services or, in the case of alteration of patient data, large-scale clinical errors.

Recent research has identified the healthcare sector as one of those exposed to the greatest risks in terms of cybersecurity, because it lacks an organic plan of security and protection, which would be essential in this field, especially in view of the increasing use of cloud computing and artificial intelligence.

In this regard, statistics confirm that the healthcare world is twice as likely, compared to other environments, to suffer from data loss or be the target of *cyber attacks*.

In particular, in the first nine months of 2019, *cyber attacks* on healthcare facilities increased by 60%.

This situation is believed to arise from the high value of patient financial and health data that the health care world processes. More precisely, the value of this type of information is linked to its depth and scope: it includes personal data, date of birth, e-mail addresses, health card numbers, employment data, medical information, insurance data.

As a result, health data has a value in the illegal market that is 10 times higher than credit card numbers and it has been estimated that the average cost of a lost or stolen data record is 136% higher for a healthcare organization than for other types of organizations[35].

As proof of this, precisely in this last period there have been *cyber attacks* linked to the health emergency, aimed at stealing as much health data as possible. And the risks increase, evidently, also due to the greater number of subjects who are called to enter data into the FSE, which, as mentioned, are not only the doctors of the regional health system, but all the health professions that take care of the patient regardless of location. This will inevitably also involve the opening of the FSE to private subjects whose systems will have to interact with the public standard, subject to compliance with the defined safety measures. And it is obvious that the involvement of a wide range of stakeholders in the health sector will also put to the test the current policies for the processing of personal data and the security of the related management systems.

Therefore, if it is true that the FSE is a highly innovative and effective tool, that technological progress makes it possible to put at the service of patients' health, it is also true that its use also entails new pitfalls for patients' right to privacy.

6. The challenges that digital health poses and the perspectives *de iure condendo.*

In light of the risks just highlighted that an "out of control" evolution of digital technology would entail, it is clear that, today more than ever, it is necessary to take note of the need for health data to be guaranteed the correctness of origin and safety of circulation.

It is believed, in fact, that only through strict compliance with the rules on privacy can we attribute the right dimension to information security, to be understood as the set of arrangements to protect all data from accidental events, preventing the vulnerability of the data contained in the various systems to continue to translate into the vulnerability of our physical life[36].

Well then: new needs, new challenges to face.

A first challenge can be considered the need to ensure, as previously mentioned, the interoperability of health data, in order to allow the obtaining of data from multiple sources and to combine them in a usable way. In this sense, a more massive and homogeneous use of the FSE tool would certainly be desirable.

Another objective can be considered the realization of systems in which there is certainty on the authenticity of the information present and available for use by the assigned different operators, so all the necessary precautions must be taken to certify the data entry process.

In addition, it should be sought to exclude the possibility that medical information be accessible and modifiable even by persons who, although part of the medical sector, are not entitled to access such files. With reference to this second challenge, it should be pointed out that the outcome of inspections carried out in recent years in the health sector, has highlighted the presence of abusive access to health records by administrative or medical

[35] *Digital Guardian: The definitive guide to Data Loss Prevention* – Healthcare Edition.

[36] E Sorrentino, AF Spagnuolo, 'La sanità digitale in emergenza Covid-19', (n 28), 250.

personnel, who had never been involved in the process of patient care and who, for reasons of personal interest, had accessed the same, and then disclosed the information thus acquired to third parties without the knowledge of the person concerned.

Finally, a final challenge can be considered protection from the risk of abusive access by hackers.

In a first step to ensure that these challenges can be accepted (and, above all, won), in a *de iure* perspective, it seems appropriate, first of all, to reflect on the fundamental choices to which our civilizations are called. In this regard, the President of the Guarantor for the Protection of Personal Data has pronounced himself, stating that, on the one hand, the IT risk (which can fatally evolve into clinical risk) must be contrasted with the strictest compliance with the principle of accountability and the criteria of privacy by design and by default, rationalizing the information heritage and the architecture of the processing itself, following the dynamics along the entire chain; on the other hand, the risk of undue access to data in the health record, made possible by an inadequate definition of the perimeter and legitimation profiles of the health professionals themselves, should not be underestimated. In this regard, the Guarantor has recently stated that cases of consultation of health records by unqualified personnel have not been rare, for retaliatory purposes or due to simple, pathological, curiosity[37].

Therefore, the spectrum of data breach should never be underestimated, because data breaches - especially in difficult times such as the current one caused by the Covid-19 emergency - are just around the corner.

One solution, if we want to defend rights and freedoms (of individuals but also of the community), could be to deploy resources on the cybersecurity and national cybernetic security front, because ever increasing information and digital heritage can jeopardize the protection and confidentiality of data processed.

In addition, "cultural" obstacles should also be overcome through the training and updating of health workers so that the health professional does not perceive ICT (Information and Communications Technology) as the fulfilment of or, worse, as a burden on his workload but, and above all, as part of a precise common strategy, the benefits of which affect the whole health system. Healthcare workers must, therefore, understand that among their duties, today, there is not only that of treating people, but also that of taking care of their data. And to this end, health data management strategies are needed to ensure that health data is always protected and available in a reliable, timely and consistent manner.

In the light of what has been said so far, it can undoubtedly be said that the digitization of healthcare is a crucial challenge for our country, with respect to which, however, its fragmentation and inhomogeneity and the absence of an organic security plan have emerged. And this can, without a doubt, represent a major cause of malpractice, making, at the same time, the protection of data and systems a decisive fact of health efficiency.

In fact, taking the FSE as an emblem of this challenge, one cannot fail to emphasize that entrusting the entire medical history of millions of patients to an IT infrastructure is also a not insignificant source of vulnerability, if it lacks adequate protection to prevent undue access, exfiltration or alteration of data: the loss, removal or alteration of health data puts at risk essential databases and, at the same time, violates the most intimate privacy of the individual person, exposing him or her to serious discrimination.

The ultimate goal, therefore, is to make digitization in health care an organic, far-sighted and safe process, thus promoting the efficiency of the system and, with it, the effectiveness of the right to health, overcoming the vulnerabilities of technology and minimizing individual

[37] 'Privacy e dati sanitari. Il Garante: "Incrementare sicurezza, non rari casi di consultazioni indebite Fse' (2020), 26 May, quotidianosanita.it.

and collective risks.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Migrants and refugees in the cyberspace environment: privacy concerns in the European approach

MIRKO FORTI
Researcher Fellow at Sant'Anna School of Advanced Studies of Pisa

Abstract

Migrants and refugees use their smartphones during their migration journey in several ways. They rely on the Internet, and more specifically social media platforms, to maintain a bond with families and friends back in the State of origin, to get information about their planned routes, to keep contacts with smugglers and traffickers and as a tool of integration in the national community of intended destination. Although smartphones are useful instruments for their migration plans, these devices could also become a gateway to digital surveillance. This article aims to focus on the relationship between smartphones and migrants and its legal consequences, especially about privacy and data protection concerns. More specifically, the study would like to individuate how the utilization of digital devices in the context of mass migration phenomena could expose migrants and refugees to several threats coming from the cyberspace dimension. Thus, it is fundamental to verify which kind of legal safeguards the European regulatory framework could provide to protect the right to privacy and data protection of these subjects.

Keywords: Migrants - Refugees - Social Media - Smartphones - Privacy - Surveillance.

Summary: Introduction. – 1. Smartphones and social media in the migration context: positive factors and possible vulnerabilities for migrants and refugees. – 2. The GDPR in the context of mass migrations: profiles of (non) regulatory compliance. – 2.1. The definition of "personal data" and the metadata problem. – 2.2. Data protection principles and digital surveillance methods for migrants and refugees: the need for a legal assessment. – 2.3. Information and access to personal data and the cultural gap regarding the concept of privacy. – 2.4. Legal basis for data processing activities in the management of mass migrations phenomena. – 3. Concluding remarks.

Introduction.

Nowadays, a smartphone is an essential part of the toolkit of every migrant ahead of the planned journey, likewise water and food[1]. ICT technologies are increasingly becoming a fundamental factor in the mass migration phenomena for several reasons. Smartphones are the ideal gatekeepers to a potentially indefinite amount of information useful to plan and enable a migration journey.

Although their undoubtful utility, electronic devices could rapidly become a tool for digital surveillance in the hands of border control authorities and also migrant smugglers. Smartphones contain personal data regarding their owners and their online activities, such as web searches, social media accounts and location data. In the migration context, surveillance methods could exploit this information to keep under control migrants, in spite of their fundamental right to privacy and personal identity.

Accordingly, the main focus of this article is to evaluate the profiles of compliance

[1] I Kaplan, 'How smartphones and social media have revolutionized refugee migration', UNHCR Blogs, https://www.unhcr.org/blogs/smartphones-revolutionized-refugee-migration/ (last seen on 27 April 2020).

between the use of smartphones and social media by migrants and refugees and the European regulatory data protection framework in order to formulate a consistent policy and legal approach to safeguard the fundamental rights of the individuals involved. The first step is to understand the real importance of ICTs in the mass migration context, focusing on the positive sides and the downfalls of using an electronic device before and during the journey.

1. Smartphones and social media in the migration context: positive factors and possible vulnerabilities for migrants and refugees.

Migrants and refugees rely on an extended digital infrastructure to plan their journey and to reach their final destination safely. Smartphones can act as an aggregator of several kinds of information and as an enabler of communication channels. Accordingly, migrants are currently using electronic devices for distinct functions which are hereby worth mentioning[2].

Firstly, the Internet can be a valuable tool for navigation and geolocation purposes. Migrants use their smartphones to be continuously updated about their journey and to receive information like the most efficient route, weather and climate conditions, border controls[3]. In the same way, Global Positioning System technology (GPS) is often used by smugglers and migrants themselves to navigate in the Mediterranean waters[4].

The deployment of these digital resources is gradually mutating the ongoing relationships in the migration context; individuals prefer to rely on these technologies and the help of fellow migrants, instead of smugglers, to find the way to the next destination while on the route[5].

Secondly, ICT technologies enable the first contact between people who are planning to move away and traffickers. Several social media groups are the digital place where smugglers can advertise[6] their services to potential customers who can compare different journey packages and prices[7]. Additionally, these virtual platforms include "reviews" of previous clients who are sharing their knowledge and experience with potentially future migrants.

The continuous flow of information regarding migration journeys and services offered by smugglers available on social networks reveals both positive aspects and possible downfalls[8]. Migrants and refugees can choose from a variety of routes and means of transport advertised on social media groups, therefore, they are able to make more secure choices. However, they often count on unreliable information considering how smugglers and traffickers are led to underestimate every risk factor regarding their journeys. Furthermore, criminals often use social networks like Facebook to sell fake passports and ID cards in order to allow migrants

---

[2] M Gillespie and others, 'Mapping refugee media journey. Smartphones and social media networks', *https://www.open.ac.uk/ccig/sites/www.open.ac.uk.ccig/files/Mapping%20Refugee%20Media%20Journeys%2016%20May%20FIN%20MG_0.pdf* (last seen on 27 April 2020).

[3] B Frows and others, 'Getting to Europe the "Whatsapp" way. The use of ICT in contemporary migration flows to Europe', (2016), 2, RRMS Briefing Paper, http://www.mixedmigration.org/wp-content/uploads/2018/05/015_getting-to-europe.pdf (last seen on 27 April 2020).

[4] J Schapedonk, D Van Moppes, 'Migration and information: images of Europe, migration encouraging factors and en route information sharing', (2007), 16, Working Paper Migration and Development Series, 1,29.

[5] R Khalaf, 'Technology comes to rescue in the migrant crisis', Financial Times, 24 February 2016, https://www.ft.com/content/a731a50a-da29-11e5-a72f-1e7744c66818#ixzz41ks4s7ZX (last seen on 28 April 2020).

[6] Reuters, 'Migrants smugglers use Facebook to promote Turkey-Italy trips bypassing sealed Balkan route', 2 April 2016, https://www.rt.com/news/338087-migrant-smugglers-italy-facebook/ (last seen on 28 April 2020).

[7] B Frows and others, 'Getting to Europe', (n.3).

[8] E Diker, 'Social media and migration', Political and Social Research Institute of Europe Blog, http://ps-europe.org/social-media-and-migration/ (last seen on 28 April 2020).

to pass border controls.

One of the several challenges faced by migrants and refugees during their trip is to understand foreign languages and to communicate with people[9]. Electronic devices can provide valuable help in this regard through websites and translating apps.

Smartphones could also act as a tool of digital witnessing of the migration journey under a double aspect[10]. Firstly, they contribute to strengthening a bond between migrants *en route* and their family and friends back in the country of origin through the sharing of multimedia contents like video, photos of every stage of the journey thus to create a sense of connection in spite of the distance. Additionally, migrants could use smartphones to record every abuse and stressful situation which they have to face during their travelling, such as human right violations[11].

In conclusion, the multimedia capabilities of smartphones and social networks are useful for migrants and refugees in many ways; as an aggregator of information, a tool to keep in contact with family, an instrument to facilitate their journey and to foster their integration in the country of destination. However, ICT's technologies could reveal vulnerable aspects regarding the fundamental rights and personal identity for the same subjects. Smartphones could rapidly become an instrument of digital surveillance according to the potentially indefinite amount of personal data contained in such electronic devices. The growing ability to track movements of persons in real-time through their digital tracks raises new profiles of threats and vulnerabilities for migrants and refugees, more specifically for their fundamental right to privacy and data protection.

Several States in the European Union are currently exploiting this possibility for security purposes or, at least, they are evaluating this kind of policy approach. Belgium recently approved specific normative provisions[12] to allow border authorities and patrols to check asylum seekers' digital devices. This approach is possible according to an extensive interpretation of the terms of the art.13.2 (d) of the Directive 2013/32/EU[13]: the norm states that "*competent authorities may*

search the applicant and the items which he or she is carrying". Likewise, the possibility to check digital profiles of migrants and refugees at border controls is at the centre of political debate in other European countries like Germany[14].

There are two different motivations behind this policy approach regarding the ways of patrolling national borders[15]. On a first basis, checking social media accounts and electronic devices could be an alternative manner to control personal identity when ID documents or passports are not available. National authorities could verify if migrants and asylum seekers

---

[9] M Gillespie and others, 'Mapping refugee', (n.2)

[10]M Gillespie and others, ibid.

[11] E Isin, E Ruppert, *Being digital citizens* (1st edition, Rowman & Littlefield Publishers, 2015) 140.

[12] Loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers, 21 November 2017, http://www.ejustice.just.fgov.be/eli/loi/2017/11/21/2017032079/justel (last seen on 28 April 2020).

[13] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection, [2013] OJ L 180/60.

[14] P Oltermann, J Hentley, 'German proposals could see refugees'phones searched by police', The Guardian, 11 August 2016, https://www.theguardian.com/world/2016/aug/11/germany-security-proposals-refugees-phones-searched-suspicious-posts-social-media (last seen on 28 April 2020).

[15] M G Jumbert and others, 'Smartphones for refugees: tools for survival or surveillance?', (2018) 4, Prio Policy Brief, 1, https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf (last seen on 28 April 2020).

have all the characteristics to ask for international protection, searching for clues and evidences on social media profiles and smartphones or laptops. Lastly, border guards look for potential threats for national security in the context of counter-terrorism actions.

Furthermore, smugglers and traffickers check social media accounts of migrants and refugees, even after the end of the journey, to not lose control over them and to maintain these subjects under the influence of criminal organizations.

In conclusion, relying on ICTs in the context of mass migrations presents a double side effect. On the one hand, it allows migrants and refugee to take more meaningful decisions during their journey and facilitate their integration in the country of destination; on the other hand, raises privacy and data protection concerns which are worth mentioning and expose worrying profiles of vulnerability regarding the sphere of fundamental rights of the people involved.

Thus, it is necessary to individuate which are the feasible normative solutions within the application sphere of the European data protection regulatory framework, especially the Regulation (EU) 2016/679[16] (hereinafter also GDPR), to safeguard the right to privacy and personal identity of every individual in the context of mass migrations.

2. The GDPR in the context of mass migrations: profiles of (non) regulatory compliance.

The Regulation (EU) 2016/679 is the core of the European regulatory framework regarding the right to privacy and data protection. Its features take into account the technological progress, which is continuously raising new challenges for privacy in the digital ages. The actions of the European Union and all the Member States in the management of mass migrations have to respect the normative provisions of the GDPR, although there should be a few problems of regulatory compliance which are worth of mentioning.

2.1. The definition of "personal data" and the metadata problem.

The concept of "personal data" is not an immutable and abstract idea, while it rapidly changes during the time to respond to the needs of an evolving society. The advent of the Internet and, therefore, the global diffusion of a communication network has radically revolutionized the traditional paradigm of privacy, introducing new digital elements capable to identify univocally a single person.

Thus, the GDPR states a broad definition of personal data, readily adaptable to the innovations of digital progress: according to art 4.1 of the Regulation, "personal data" means any information relating to an identified or identifiable natural person called data subject.

Focusing on digital surveillance methods regarding migrants and refugees, the GDPR does not declare anything regarding the so-called metadata[17]. This term indicates the "data about data", namely data reporting information about one or more aspects of data, allowing faster and easier processing of data itself. Metadata, if considered singularly, are inherently anonymous, so they are not able to indicate univocally a single individual. They need to be combined together to point out the above data subject. Thus, the GDPR applies only to aggregated metadata, although illegitimate processing of such information could seriously

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.

[17] R Guenther, J Radebaugh, 'Understanding metadata', National Information Standard Organization (NISO), 2014, https://web.archive.org/web/20141107022958/http://www.niso.org/publications/press/UnderstandingMetadata.pdf (last seen on 30 April 2020).

harm the right to privacy of everyone involved. Metadata could reveal important information about specific individuals and their online behaviour without plainly identifying any data subject; for example, indicating when and where a specific digital resource was created. If adequately processed, metadata could point out habits and intentions of migrants and refugees during their journey. National authorities could process metadata when inspecting laptops and smartphones at border checks, although GDPR may not provide sufficient safeguards for the right to privacy of people involved regarding this type of information. Proposals for reforming the ICT legal framework would probably entail metadata too. The forthcoming Regulation ePrivacy[18] would allow the processing activities of metadata only in case of previous approval of the involved data subject. The metadata issue is one of the main topics at stake in the current debate about such reform effort[19]. The scope of the GDPR is not limited to defining the concept of "personal data". Regulation 2016/679 lists a series of founding principle which every data processing activity shall follow.

2.2. Data protection principles and digital surveillance methods for migrants and refugees: the need for a legal assessment.

Principles of fairness, lawfulness and transparency must characterize every data processing activity (art.5.1a GDPR). Moreover, personal data shall be collected only for *specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes* (art.5.1b GDPR). Information shall be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed* (art.5.1c GDPR) and *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed* (art.5.1e GDPR). Lastly, the controller shall be held accountable for the data processing activities conducted under his/her control (art.5.2.GDPR).

According to these normative provisions, the main question is if the digital surveillance methods, like checking social media accounts and digital devices, used by national authorities in the management of mass migrations phenomena could comply with the fundamental principles of GDPR.

European governments are increasingly focusing their attention to the ICTs environment during border controls, in order to find out every possible evidence of national security threat "hidden" in the digital activities of migrants and refugees. There is a strong convincement that the wealth of data stored in electronic devices can indicate without any possibility of doubt or mistake the "real identity" of the owner of the laptop or the smartphone[20]. However, this is not a self-evident truth for several reasons, especially concerning migrants who are fleeing away from dramatic situations like war zones[21].

For instance, Islamic State agents and Syrian guards often request Facebook passwords during checkpoint controls to verify the allegiance of the subject during the civil war[22]. Accordingly, individuals may have changed their online habits to prevent arbitrary allegations derived from any kind of intrusion in their digital private sphere. Moreover, several people

---

[18] Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

[19] T Ricci, 'Regolamento ePrivacy: a che punto siamo e cosa aspettarsi con la presidenza tedesca', 30 October 2020, https://www.agendadigitale.eu/sicurezza/privacy/regolamento-eprivacy-eppur-si-muove-a-che-punto-siamo-e-cosa-aspettarsi-nel-2020/ (last seen on 13 November 2020).

[20] M G Jumbert and others, 'Smartphones for refugees' (n.15)

[21] M G Jumbert and others, ibid.

[22] M.Brunwasser, 'A 21st-century migrant's essentials: food, shelter and smartphone', The New York Times, 25 August 2015, https://www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=1 (last seen on 30 April 2020).

may have used the same device, which, therefore, would contain mixed digital trails originated from different subjects. Not every migrant has a smartphone during the journey and it could happen to lose the electronic device or to run out of battery. In light of the above considerations, government authorities should assess data collected from migrants' digital tools very carefully, not acritically assuming their trustworthiness and taking into appropriate account the context in which data are developed. Thus, it is questionable the effectiveness of this kind of border controls and therefore their legitimacy, considering how they may not provide reliable evidence regarding the online habits of the migrant.

Furthermore, it is likewise doubtful the compliance of these digital surveillance methods with the principles of data minimisation and purposes limitation, considering how the amount of data collected may not serve to reach the scope of identifying migrants and their future actions.

Data processing activities shall enshrine the above-mentioned principles but, to be effective, they shall take into account the cultural divergencies of people involved in such procedures.

2.3. Information and access to personal data and the cultural gap regarding the concept of privacy.

One of the fundamental cornerstones of the European regulatory framework of privacy is the right to information and access to personal data (Art 13-15 GDPR). More specifically, the controller shall provide the data subject with all the information related to the processing activities (purposes, the legal basis etc.) Furthermore, the data subject is entitled to know every feature regarding the ongoing processing of his/her personal information.

The rationale behind these normative provisions is to allow the data subject to maintain a sort of control over his/her own personal data; in the digital age, the concept of privacy is gradually overlapping with the idea of informative autonomy[23]. The traditional paradigm of privacy intended as "*the right to be let alone*[24]" has no more room in the cyberspace era: everyone is permanently connected to the Internet network, continuously sharing personal data thus it is no more possible to individuate a completely intimate sphere for the individual. The right to data protection is nowadays integrating the scope of application of the concept of privacy, in order to allow the data subject to have full disposal about the own information shared[25].

However, the idea of "*right to be let alone*" is not inherently abstract, but it founds its own roots in a specific western societal background. The right to privacy was a sort of corollary to the right to private property, which was the founding core of the European and American society in the first years of the last century; any intruder is not allowed to enter the home (private sphere) of an individual without his/her permission. Thus, the right to privacy found its rationale through an individualistic perspective as a tool to permit the self-fulfilment of every subject[26], although it may cause contrasts with the needs of the entire collectivity[27].

However, the idea of privacy is too elaborated and multifaceted to be reduced to a single static concept[28], not considering the several influences of different cultural backgrounds.

In light of the mass migrations context, it is therefore worth mentioning the role of

---

[23] S. Rodotà, *Tecnologie e diritti,* (1st edition, Il Mulino,1995) 19.
[24] S D Warren, L D Brandeis, 'The right to privacy'*,* (1890) 4, Harvard Law Review, 193.
[25] A.F.Westin, 'Privacy and freedom'*,* (1968) 25:1, Washington and Lee Law Review, 166.; L.Lusky, 'Invasion of privacy: a clarification of concepts', (1972) 87:2*, Political Science Quarterly,* 192.
[26] A F Westin, ibid.
[27] P.M.REGAN, *Legislating privacy:technology, social values and public policies,* (5th edition, NCUP, 1995) 212.
[28] D J Solove, *Nothing to hide: the false tradeoff between privacy and security,* (10th edition, YUP, 2011) 24.

privacy in the African society in order to bridge the cultural divide between European immigration officers and migrants coming from the African continent[29] regarding the needed information to share.

Societies not characterised by an individualistic perspective may difficultly accept the concept of privacy as elaborated through the western experience[30].

The traditional representation of African society sees the individual as a part of the entire community and not as a single unit with autonomous needs and aspirations[31]. Ubuntu philosophy thinking, typically originated in African countries, puts at the top of the social pyramid the group, which could be for instance the family, the clan or the tribe; the self-fulfilment of the subject is subordinated to the needs of the above-mentioned group of membership[32]. There is no space for a concept of privacy as intended in the western world, as an intimate sphere outside of the public collectivity.

Thus, it is understandable why the African Charter on Human and Peoples' Rights, a regional treaty on fundamental rights, does not clearly state a right to privacy[33].

However, African culture is not static, but it is in constant motion and evolution[34]. The Internet network is rapidly growing through the entire continent, and African cyberspace users are currently experiencing the same challenges to their right to data protection of European and American citizens. Moreover, socio-economic factors like the growing urbanization, which is characterizing the African continent nowadays, is radically transforming the traditional paradigm of societal aggregation based on the basic unit of the social group for a more individualistic point of view. Farms and small factories run by families are giving way to industrialization approach inspired by the western model[35].

In conclusion, the concept of privacy is present in the African culture, although with peculiar features compared to the Western way of thinking. The focus is not only on the individual but on the subject in relationship with the entire collectivity.

Thus, immigration officers should consider these peculiarities in approaching migrants just arrived in Europe from Africa, knowing which kind of data are these people willing to share with European national authorities. Moreover, several interviews on the field report how migrants are often confused regarding sharing personal information about themselves without knowing the reasons behind these data processing activities[36]. Migrants should overcome language and cultural barriers, to not mention the shock of a long and perilous journey, to fully understand the bureaucratic practices behind the migration management activities and, more specifically, identification process.

In light of the above-mentioned considerations, it is highly questionable if migrants can really enjoy a proper right to access and information as stated by the GDPR.

Moreover, they are pushed to share their personal data also for humanitarian purposes:

---

[29] M Latonero and others, 'Digital identity in the migration and refugee context. Italy case study', https://datasociety.net/library/digital-identity-in-the-migration-refugee-context/ (last seen on 2 May 2020).

[30] L A Bygrave, '*Privacy protection in a global context – A comparative overview*', (2004) 47, Scandinavian Studies in Law,139.

[31] E.J Lassiter, '*African culture and personality: bad social science, effective social activism or a call to reinvent technology?*', (2000) 3, African Studies Quarterly,1

[32] M N Kamwangamalu, 'Ubuntu in South Africa: a sociolinguistic perspective to a Pan-African concept', (1999) 2, Critical Arts: South-North Cultural and Media Studies, 24

[33] African Charter on Human and Peoples' Rights (Banjul Charter), 28 June 1981, https://www.achpr.org/legalinstruments/detail?id=49 (last seen on 3 May 2020).

[34] L.A.Bygrave, 'Privacy and data protection in an international perspective', (2010) 56, Scandinavian Studies in Law, 176.

[35] A B Makulillo, '"A person is a person through other persons" – A critical analysis of privacy and culture in Africa' (2016) 1, Beijing Law Review,192.

[36] M Latonero and others, 'Digital identity' (n.27).

NGOs and national authorities operating on the field need to identify every single subject to provide everyone with fundamental help, namely food and medical treatments. Do migrants have a real choice in deciding when and how to give their own information or not? Is consent a suitable legal basis for data processing activities in the mass migration context?

2.4. Legal basis for data processing activities in the management of mass migrations phenomena.

The GDPR sets out a list of alternative legal grounds based on which processing data activities are considered lawful (art.6). One of the options is when the data subject has given *consent to the processing of his or her personal data for one or more specific purposes*. The controller has the legal duty to demonstrate that a free, informed and specific consent has been effectively provided. Moreover, the data subject can withdraw at any moment his/her consent previously stated without incurring in any legal or technical obstacle (art.7).

Thus, national authorities shall respect these legal requirements in the context of mass migrations management, even though it could be not a simple task to guarantee these rights to migrants and refugees and, more specifically, regarding digital data and online activities trails.

Firstly, there is a language and cultural barrier to overcome to reduce the understanding gap between immigration officers and migrants. As mentioned before, the concept of privacy could have several meanings and features according to the different cultural backgrounds, therefore, people could utilize non-identical words to define this idea. There is plenty of room for misunderstanding, although the GDPR affirms the principle of transparency as a fundamental one. Migrants cannot provide valuable consent if they do not understand the administrative procedures of collecting their personal data.

NGOs and national authorities need to identify every person before providing them with fundamental help, namely food, water, medical treatment[37]. Thus, migrants are in front of an apparent dilemma: to provide every data asked to receive help for their basic needs or to maintain a sort of control over their own personal and digital identity? The answer is obvious and self-evident.

A disproportionate relationship between immigration officers and migrants could not lead to choosing free consent of the data subject as a legal basis for data processing activities[38].

Furthermore, border guards should consider another important factor before identifying every individual: the state of shock and psychological distress mixed with the relief of being saved from the perilous journey would not allow migrants to understand which kind of data are sharing and for which purposes[39].

In light of the above considerations, it could happen that consent would not be a suitable legal basis for data processing activities on many occasions in the context of mass migrations, due to the specific vulnerabilities of the data subjects involved. Thus, the GDPR states other possible legal grounds and, for the purposes of this study, are particularly important the vital interest of the data subject or another natural person (art.6.1d) and the public interest of the collectivity (art.6.1e)[40].

It is undisputable the interest of the migrants in receiving help, even though this assistance would mean processing their personal data for identification purposes. However, this legal

---

[37] C.Kuner, M.Marelli, 'Handbook on data protection in humanitarian action', 2020, https://www.coe.int/en/web/data-protection/-/new-handbook-on-data-protection-in-humanitarian-action, (last seen on 12 November 2020).

[38] M Latonero and others, 'Digital identity' (n.27).

[39] M Latonero and others, ibid.

[40] C.Kuner, M.Marelli, 'Handbook on data protection' (n.35).

basis can legitimate only actions directed to provide help to migrants. Furthermore, data subjects should be informed about their right to object and to request the privacy policy which illustrates the modalities and goals of the data processing activities.

It is likewise unquestionable how the correct management of the mass migrations phenomena is a matter of public interest. Nevertheless, the data subjects should be made aware as soon as possible of every data processing activity regarding their identity and about their privacy rights.

Focusing more specifically on the scope of this study, it is worth questioning the legitimacy of digital surveillance procedures concerning the online trails on electronic devices and social media accounts. Although the legitimate interest of the European Union to identify every subject arrived into its territory in the context of migration flows is surely understandable, inspecting smartphones and laptop may not be compliant with the fundamental rights of people involved. Consent may not be a suitable legal basis, because it is not technically possible to previously inform migrants involved in these controls about the type of data which will be found in the electronic device (metadata, geo-localization indicators etc).

Even considering the legal obligation of every State to preserve the integrity of their own borders and the national security of their citizens, the data subject has the right to be informed as soon as possible regarding the data processing activities and the possibility to object: is this feasible in the context of similar digital controls?

3. Concluding remarks.

Although they can go unnoticed, migrants and refugees are inhabitants of the cybernetic dimension with specific needs and necessities worthy of attention. They use information and communication technologies to share experiences about their migration journeys, to acquire knowledge regarding their future destination and all the administrative and bureaucratic procedures to enter into the European Union and to maintain a bond between them and their family back in their homeland.

However, their online activities could expose their digital identities to relevant dangerous threats in terms of privacy and data protection vulnerabilities. Smugglers and human traffickers could utilize these virtual tracks to maintain a sort of illicit control over these people, even after the end of the migration journey. Furthermore, criminal organizations constantly use social networks to make the first contact with people interested in reaching the European territory in an illegal manner.

Additionally, a few European States are focusing their attention on how to exploit virtual trails left by migrants during their permanence in the cyberspace dimension to establish digital surveillance methods to protect their national borders. Border patrols could inspect electronic devices to find out possible evidence of national security threats.

\The European regulatory approach should reach a balance between the legal obligation of every State to preserve the integrity of the national borders and the safeguards to the rights of privacy and data protection of every individual, including migrants.

The fundamental basis of the European regulatory framework in this regard, the GDPR, does not explicitly state any normative provision about the collection of personal data in the management of mass migrations context[41], although the relevant peculiarities of this field.

Thus, one of the goal of this study is to point out the most relevant profiles on non-compliance between the GDPR norms and the digital control procedures regarding migrants and refugees. Firstly, it stands out how these surveillance methods may not respect the

[41] M Latonero and others, 'Digital identity' (n.27).

fundamental principles of transparency and proportionality. It is not always possible to individuate exactly which kind of data national authorities collect from the cyberspace to identify every migrant. Furthermore, it is disputable the real necessity of this kind of controls, considering how misleading could these digital data be. For instance, migrants could modify their online habits to avoid being surveilled by national authorities. Furthermore, it is not unusual that different subjects could use the same device during the migration journey, making therefore impossible to individuate which individual the data are indicating.

However, the study of the regulatory compliance of these digital surveillance methods with the GDPR is only the first step to address the fundamental issue of the right to digital identity for migrants and refugees.

Every individual holds the right to personal identity[42] and to be not discriminated in front of the Law[43], even though these words could be not applied in reality[44] due to the lack of valid proof of legal identity[45]. For instance, asylum seekers need ID cards or whether identification documents would not be able to acquire legal status in the destination country[46]. In this regard, technology could provide useful tools to identify every individual, even the ones without legal ID documents, and therefore enable them to enjoy the same opportunities of the rest of the citizens[47].

However, relying on technological means for identification purposes could expose migrants and refugees to several threats concerning possible discriminations and abuses[48]. Technology tools are neutral instruments; thus, they are not aprioristically "good" or "evil", but depending on their utilization in the hand of human beings. They can provide valuable help in reaching non-discrimination goals, but they can also be used for discriminatory practices[49] such as tailored surveillance methods.

States should use digital data collected exclusively for the aim to identify migrants and not to establish abusive surveillance controls: national authorities are legally obliged to reach a balance between the State's and the individual's interests[50]. Accordingly, identity platforms providers should design their software in light of the regulatory framework concerning privacy and data protection and focusing on the specific context of mass migrations to adequately safeguard the right to digital identity of migrants and refugees.

In this regard, the GDPR introduces the concepts of privacy by design and privacy by default (art.25) which can act as useful guidelines in preventing digital abuses and data breaches[51]. According to these principles, providers shall implement, since the very first phases of the data processing activities, all the appropriate measures to safeguard the fundamental rights of every data subject in light of the specific peculiarities of the context.

Besides implementing the necessary technical and legal measures, the European Union,

---

42 Art.6 Universal Declaration of Human Rights; Art.16 International Covenant on Civil and Political Rights.

43 Art.1,2,7 Universal Declaration of Human Rights: Art.26 International Covenant on Civil and Political Rights.

44 S Friedman, 'Substantive equality revisited' (2016)14, International Journal of Constitutional Law, 712.

45 A Beduschi, 'Digital identity: contemporary challenges for data protection, privacy and non-discrimination rights', in,(2019)1, Big Data and Society,1.

46 A Beduschi, ibid.

47 M J Haenssgen, P Ariana, 'The place of technology in the capability approach', (2018) 46, Oxford Development Studies, 98.

48 A Beduschi, 'Digital identity: contemporary challenges'(n.43)

49 A Beduschi, ibid.

50 European Court of Human Rights, Judgement 4 December 2008, *S.and Marper v.United Kingdom,* application n.30562/04, 30566/04

51 A Rachovitsa, 'Engineering and lawyering privacy by design: understanding online privacy both as a technical and an International human rights issue', (2016) 24, International Journal of Law, Information and Technology, 374.

alongside all the member States, should move forward in the management of mass migration phenomena also under a cultural and societal perspective. Nowadays, migrants and refugees do not trust the administrative procedures of identification at the European borders: they believe that sharing their personal data, they would be under constant digital surveillance. Therefore, they try to avoid any form of control, modifying their online habits and refusing to share their information. In this way, they firstly harm themselves; they are not able to integrate into the European community suffering from the exclusion from the cyberspace context. In a few words, they are not free citizens and therefore possible victims of criminal organizations.

To conclude, a working European regulatory and policy approach should clearly understand the fundamental importance of ICTs technology for migrants and refugees, both as survival tools during the migration movement and as instruments of integration, to bridge the digital and cultural gap in terms of privacy and data protection between the European world and the African and Middle East lands.

EJPLT

Consideration of privacy aspects in the area of highly automated driving. An intention recognition use case

LIVIA AULINO
Ph.D. Candidate at the University Suor Orsola Benincasa of Naples
MARCEL SAAGER
M.Sc., Modelling & Software Engineer at Humatects GmbH
MARIE-CHRISTIN HARRE
HMI Engineer at Humatects GmbH
LEONARDO ESPINDOLA
Industrial Designer at Humatects GmbH[1]

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Abstract

Autonomous driving is increasingly becoming an issue in the development of modern vehicles. Above all, aspects such as safety and comfort are encouraging carmakers to embed highly automated driving in their latest developments. Due to the increasing complexity and the fact that it is often not clear how and for what purpose user data is processed, it is important to take a closer look at the legal and data protection aspects. For this purpose, a use case has been selected from the AutoMate project, on the basis of which current case law is to be applied in an exemplary manner.

Keywords Autonomous driving - Data processing - Data protection law - Human-Machine Interaction

Summary: Introduction. – 1. The Use Case: Intention Recognition. – 2. Related Work: Legal Aspects in the field of highly automated driving. - 3. Privacy Aspects in the underlying use case. – 3.1. First Phase: to set up whether the processing of the collected data falls within the scope of the GDPR. – 3.2. Second Phase: to apply GDPR regulation, if the data collected are not anonymous. – 3.3 How to ensure that the processing is in compliance with the GDPR. – 3.4. Third phase: to set up whether it is also necessary to collect a consent of data subjects. – 4. Data processing in AutoMate. – Conclusions.

Introduction.

The latest developments in the field of autonomous driving are progressing rapidly[2].

In order to make autonomous driving possible, many values must be recorded by sensors and processed by the automation system. Sensitive data is often collected in this process, which reflects information about the driver and his or her user behavior[3].

For this reason, it is particularly important to consider not only technical advances in the

[1] Livia Aulino wrote paragraphs n. 2 - 3 - 3.1 - 3.2 - 3.3 - 3.4; Marcel Saager wrote Introduction and paragraphs n. 1 - 4; Marie-Christin Harre wrote Introduction and paragraphs n. 1- 4; Leonardo Espindola designed Figure 1 and Use Case. This paper comes from the research activity carried out by PhD. candidate at University Suor Orsola Benincasa with members of Research center Humatects (*https://www.humatects.de*).

[2] J Janai, F Güney, A Behl, A Geiger, 'Computer Vision for Autonomous Vehicles: Problems, Datasets and State of the Art', (2020) in *Foundations and Trends® in Computer Graphics and Vision*, 12:1–3, 1,308.

[3] J Varghese, RG Boone, 'Overview of Autonomous Vehicle Sensors and Systems. Overview of Autonomous Vehicle Sensors and Systems' (2015).

field of autonomous driving, but also legal aspects. Examples for the applications of these systems range from software in the aviation domain over shipping to vehicles[4].

This paper will look at the legal aspects of recording and processing sensor data for autonomous driving in more detail: a use case from the "AutoMate" project is used for this purpose.

This use case will be described in the following paper. Afterwards, the legal aspects and in particular privacy aspects of the use case will be considered in detail. The paper concludes with an examination of the problems related to the collection and processing of data inside the vehicle, and with a proposed solution for the use case.

1. The Use Case: Intention Recognition.

The use case considered in this paper originates from the european project "AutoMate" (*www.automate-project.eu*). AutoMate aims at developing the so-called "TeamMate" car in which driver and automation have to be considered as team members who share the driving task and who are both responsible for the safety of driving[5]. The scenario deals with a use case in which the fictitious person named Peter drives along a narrow rural road in Manual Mode.

The scenario is exemplarily shown in Figure 1 on the left. Peter approaches a tractor, that causes limited visibility on the road. The TeamMate car detects a car approaching from the opposite lane.

Since Peter is not aware of the car, he decides to overtake, and the TeamMate car detects his intention. In order to avoid an imminent collision, the TeamMate car informs Peter about the approaching vehicle and warns him about the risky manoeuvre. This is shown in Figure 1 on the right side. Peter suddenly becomes aware of the risk, and he does not perform the overtake until it is safe[6].

This use case was selected because it can be addressed highly autonomously driving and it can be investigated to what extent and whether user data is collected and processed.

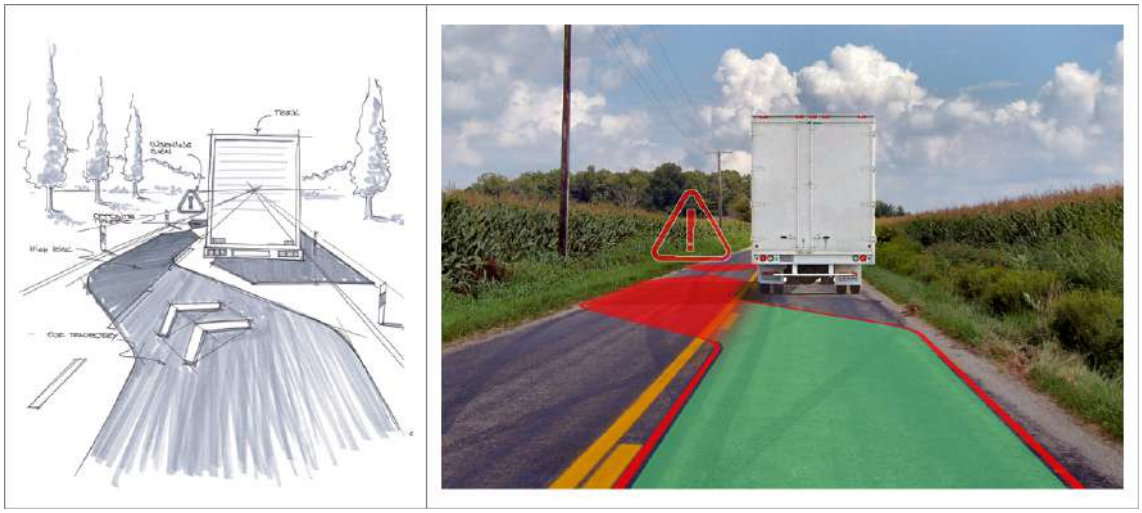


Fig.1: The Scenario.

[4] V Ilková - A Ilka, 'Legal aspects of autonomous vehicles - an overview' (2017) *Proceedings of the 2017 21st International Conference on Process Control* (Strbske Pleso 2017), 6-9, 428,433.

[5] AutoMate: Automation as accepted and trusted TeamMate to enhance traffic safety and efficiency, Website: *www.automate-project.eu*.

[6] MR Endsley, 'Situation Awareness in Future Autonomous Vehicles: Beware of the Unexpected' in *Proceedings of the 20th Congress of the International Ergonomics Association* (IEA 2018).

The Use Case considered here is situated in highly automated driving. This means in *highly automated driving* the vehicle has its own intelligence that plans ahead and can take over the driving task from humans in most situations.

Human and machine control the vehicle together, but the human driver can determine at any time to what extent he or she or the artificial intelligence takes over tasks. Examples of this are ESP and ABS. In contrast to that, *driving assistance systems* must be delimited.

They are additional modules in vehicles that are intended to support the driver in certain situations. The control is not relinquished. The focus is on safety and driving comfort. One example of this is the parking aid, which can support the driver in the process with the help of acoustic feedback.

The SAE International, Society of Automotive Engineers, defines further levels of driving modes, which will be described in the following. *Partial Driving Automation* is defined as advanced driver assistance systems that can take over steering and acceleration, for example.

Nevertheless, the human driver can intervene from the driver's seat at any time and take total control of the vehicle.

With *Full Driving Automation*, the vehicle takes over the entire dynamic driving task. Human attention and situational awareness are no longer necessary. There are currently no fully automated vehicles for normal road traffic[7].

2. Related Work: Legal Aspects in the field of highly automated driving.

The success of autonomous driving will depend on the ability to create a solid human-machine team as well as on the quality of interaction, communication and cooperation. This cooperation fully exploits the potential of automation to improve human life.

The interface also provides legal information the driver needs and precisely on: privacy and data protection (security of the data processed; lawfulness of processing; ownership); shared control (visual icons that tell the user the possibility of a risk); support and mutual learning.

The interfaces should not only content the legal and ergonomic technical needs but should also consider the experience and quality of the interaction. These should be understandable and easy to use.

Therefore, the design of interfaces requires a multidisciplinary approach that combines law, design and technology. This approach ensures that information is provided in a legal manner and in compliance with technical and HMI requirements.

In this perspective it is believed that the legal design[8] methodology is the most suitable in the design of sensor systems of autonomous driving, in order to guarantee their self-awareness. This methodology represents a possible remedy to the communication deficit of legal information provided in the car.

In fact, the solution can be seen in the opportunity to design human machine interfaces, which - also through a signalling acoustic, visual or tactile - provide legal information clearly

---

[7] SAE Standards News: J3016 automated-driving graphic update, Website: *https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic.*

[8] The notion of legal design was coined by Margaret Hagan. Legal design is the application of human-centred design to the world of law, in order to promote the usability and comprehensibility of legal instruments, and in particular contracts. Legal design is a method of creating legal services, focusing on their usability, utility and involvement. It is an approach with three main resource groups - process, mentality and mechanics - to be used for legal professionals. These three resources can help conceive, build and test better methods of legal action, which will involve and empower both legal professionals and individuals. The design phases of this methodology are: framing the situation; focusing on the type of user/consumer; developing ideas; understanding and prioritizing; developing a prototype; testing. See M. Hagan, 'Law by Design' (Retrieved March 2018), in *www.lawbydesign.co/en/home/*

and unambiguously on the autonomous vehicle. This in order to guarantee a security by design and to ensure support and mutual learning between the car and the user.

Incorporating legal regulations into the design phase can improve - or automate - their ex ante application. Thus, the problem of technological development that often hinders the regulatory efforts of legislators can be prevented. It might seem like a complex change, but it is actually easier to adopt adequate protection solutions from the start than to apply privacy considerations after a project is fully developed

The use case in question needs an in-depth study on the processing of data operated by the TeamMate car.

3. Privacy Aspects in the underlying use case.

The reference legislation is General Data Protection Regulation (Reg. UE 679/2016 – GDPR)[9], which has been in force since 2018 in all EU member States. It applies in any case where data processing in the context of connected vehicles[10] involves processing personal data of individuals.

Additionally to regulations provided by the GDPR, we can find other standards in the "ePrivacy" directive (2002/58/EC, as revised by 200/136/EC), a directive that is aimed to discipline all those actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the European Economic Area (EEA).

But, even if it is true that most of the "ePrivacy" directive provisions (art. 6, art. 9, etc.) is tailored for and only applies to providers of publicly available electronic communication services and providers of public communication networks, however we can find a general provision in the art. 5 of the ePrivacy directive. In fact, it does not only apply to electronic communication services but also to every entity that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed.

As a predictable result, a connected vehicle, and every device connected to it, shall be considered as a terminal equipment (just like a computer, a smartphone or a smart TV) and, following this statement, provisions of art. 5 ePrivacy directive must apply where relevant.

A number of issues need to be analysed in relation to the use case in question.

The first concerns establishing whether the processing of the data collected falls within the scope of the GDPR.

3.1. First Phase: to set up whether the processing of the collected data falls within the scope of the GDPR.

First of all, it is necessary to clarify what is meant by personal data.

Recital 26 of GDPR states that *the principles of data protection should apply to any information*

[9] The General Data Protection Regulation No. 2016/679, hereinafter GDPR (General Data Protection Regulation) is the European legislation on privacy and protection of personal data. It was published in the European Official Journal on 4 May 2016, and entered into force on 24 May 2016, but its implementation took place on 25 May 2018. Its main purpose was to harmonise the rules on the protection of personal data within the European Union.

[10] According to the European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, adopted on 28 January 2020, the connected vehicle definition has to be understood as a vehicle equipped with many electronic control units (ECU) that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle. As such, data can be exchanged between the vehicle and personal devices connected to it, for instance allowing the mirroring of mobile applications to the car's in-dash information and entertainment unit. Also, the development of standalone mobile applications, meaning independent of the vehicle to assist drivers is included in the scope of this document since they contribute to the vehicle's connectivity capacities even though they may not effectively rely on the transmission of data with the vehicle.

concerning an identified or identifiable natural person[11].

Most data associated with connected vehicles will include technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tyre pressure). At present, the EDPB[12] has identified three categories of personal data warranting special attention, by vehicle and equipment manufacturers, service providers and other data controllers: location data, biometric data (and any special category of data as defined in art. 9 GDPR) and data that could reveal offences or traffic violations.

More specifically the personal data could be processed inside the vehicle, exchanged between the vehicle and personal devices connected to it (e.g., the user's smartphone) or collected within the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.

Also, the Article 4 of GDPR states that 'personal data' is *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Therefore, non-anonymous data fall within the scope of the GDPR.

So if the data used in the AutoMate project were completely anonymous and not attributable in any way, neither directly nor indirectly to a natural person, then the GDPR does not apply.

Consequently, there is no need to release the privacy information and collect consent to data processing.

3.2. Second Phase: to apply GDPR regulation, if the data collected are not anonymous.

More generally, the paper examines the case in which the data collected and processed were not anonymous but were equipped with any information "*attributable directly or indirectly to a natural person*", in this case, the GDPR applies.

In this regard, the Articles 1[13] and 4,1[14] paragraph states that in the Regulation there are

---

[11] Recital 26 of GDPR: *The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.*

[12] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, adopted on 28 January 2020.

[13] Article 1 of GDPR: *1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.*

[14] Article 4,1 of GDPR: "*personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

the rules relating to the processing of personal data, that means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

For example, the data that can be traced through some encryption (e.g. if the user is identified with a number) are not anonymous.

Consequently, if the data were pseudonymous, it is necessary to understand whether data processing is ongoing.

In particular, according to the recital 18[15] and article 2,2, c)[16], the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. This includes the case where the vehicle collects personal data, but is not passed on to third parties. In this case, the data are processed only for personal purposes. Therefore, it is not a processing for which the principles of the GDPR apply, as provided for in recital 18 and art. 2 of the same Regulations.

It is different if the data are not processed exclusively by the owner of the vehicle, but in some way by a third party. In this case it falls within the concept of treatment, as laid down in Article 4, paragraph 2[17].

Once it is established that there is an ongoing processing, then it is necessary to understand who are the subjects of the processing. More specifically:

- The data subject is the natural person owning personal data. So the data subject is not only the owner of the vehicle, but it is also anyone who provides their personal data, using the vehicle. In the context of connected vehicles, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle[18].
- The data controller, according to article 4, 7 of GDPR is *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*, that take place in connected vehicles.

Data controllers can include service providers that process vehicle data to send the driver

---

15 Recital 18 of GDPR: *"This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities".*

16 Article 2 of GDPR - Material scope: "*1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Regulation does not apply to the processing of personal data: a) in the course of an activity which falls outside the scope of Union law; b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; c) by a natural person in the course of a purely personal or household activity; d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. 3.No data shall be adapted to the principles and rules of this Regulation in accordance with Article 98. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal. 4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive*".

17 Article 4,2 of GDPR: *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

18 As it was identified by European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, adopted on 28 January 2020.

traffic-information, eco-driving messages or alerts regarding the functioning of the vehicle, insurance companies offering "Pay As You Drive" contracts, or vehicle manufacturers gathering data on the wear and tear affecting the vehicle's parts to improve its quality[19].

In addition, it is necessary to understand whether the processing complies with the principles of the GDPR. The data of data subjects could be collected and processed also by more than one third party and in this case, it will be necessary to establish the role of these subjects.

Therefore, it will be necessary to determine whether it is:

- Joint controllers are two or more controllers jointly that determine the purposes and means of processing (art. 26 of the GDPR[20]). In this case, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of information as referred to in art. 13 and 14 GDPR.
- Or a data processor who manages the data in the interests of the data controller. According to the article 4,8 the 'processor' is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

E.g. the data could be collected and processed not only by the vehicle manufacturer but also by a third party (e.g. a research centre) which is responsible for the development of vehicle technologies. As another example, in several cases, equipment manufacturers and automotive suppliers may process data on behalf of vehicle manufacturers (which does not imply they cannot be a data controller for other purposes). In addition to requiring data processors to implement appropriate technical and organisational measures in order to guarantee a security level that is adapted to risk, the art. 28 GDPR sets out obligations of data processors.

For this reason, it is important to establish the roles of the various entities also in order to guarantee the rights of the data subjects and to provide the related information.

3.3 (Cont.) How to ensure that the processing is in compliance with the GDPR.

For the processing is in compliance with the GDPR it is necessary that:

- the data controller must provide the information to the data subjects. The article 12 of the GDPR provides that the data controller adopts appropriate measures to provide the data subject with all the information referred to in articles 13[21] and 14

---

[19] *Ibidem.*

[20] Article 26 of GDPR - Joint controllers: "*1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects. 2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject. 3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers*".

[21] Article 13 of GDPR: Information to be provided where personal data are collected from the data subject. "*1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*
(a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they

and in the communications pursuant to arts. 15 to 22 and to the art. 34 relating to processing in a concise, transparent, intelligible and easily accessible form, with simple and clear language, in particular in the case of information specifically intended for minors[22].

- the rights of data subjects must be guaranteed and precisely: right of access by the data subject; rectification and erasure; right to rectification; right to erasure ('right to be forgotten'); right to restriction of processing; notification obligation regarding rectification or erasure of personal data or restriction of processing; right to data portability; right to object and automated individual decision-making; right to object; automated individual decision-making, including profiling.
- In addition, the data controller must provide adequate security measures to ensure the protection and safeguard of the right processing.

In fact, according to the article 5, par. 1, lett. f) of GDPR[23], the security of the entire processing must be guaranteed, not just the data as a final product. Furthermore, article 32[24] establishes some fundamental principles on security measures, specifying that they must be adapted to the individual situation. In particular, security measures are divided into two categories: organizational measures and technical measures (such as pseudonymisation and encryption of personal data and security requirements)[25].

---

have been made available. 2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. 4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information".

[22] IA Caggiano, '*Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*' (2018) *Familia* 3,23.

[23] Article 5, par. 1, lett. f) of GDPR: "*Personal data shall be: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*".

[24] Article 32 of GDPR - Security of processing: "*1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of* personal *data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for* regularly *testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law*".

[25] F Pizzetti, *Privacy ed il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/48 al nuovo Regolamento europeo*, (Giappichelli 2016) 153.

The European regulation takes an approach based on risk assessment rather than user protection. Therefore, a correct risk analysis of the processing of personal data is appropriate in order to implement adequate security measures[26].

Consequently, in case of data processing, the information had to be provided and must be guaranteed the rights of the data subject, by articles 15 to 22.

In general, the data controller must also act in accordance with the principles of "privacy by design and privacy by default" introduced by the GDPR[27]. According to these principles it would be appropriate to provide that the technologies underlying the connected vehicles are made (from the design phase) in such a way as to minimize the collection of personal data and to ensure that the data subjects, in addition to being adequately informed, to be able to easily change any setting associated with the personal data.

In this regard it should be noted that, at the national level, the German Federal Data Protection Act of 1990, predating the GDPR, already came close to this principle. In fact, the third section of the law, named "*Datenvermeidung und Datensparsamkeit*"[28] (deletion of data and data economy), established to design information systems with the aim of processing as little personal data as possible. Furthermore, it stated that personal data must be pseudonymised or anonymized as far as reasonable in relation to the desired level of protection.

3.4. Third phase: to set up whether it is also necessary to collect a consent of data subjects.

The paper will present what the legal basis of the data processing is.

Processing shall be lawful only if and to the extent that at least one of the following applies provided by article 6[29].

---

[26] Art. 32, par. 2, lists some types of risk: accidental or unlawful destruction or loss of data; modification; unauthorized disclosure; accidentally or illegally or not authorized access.

[27] G D'Acquisto - M Naldi, *Big Data e Privacy by Design* (Giappichelli 2017).

[28] § 3a Datenvermeidung und Datensparsamkeit - Bundesrepublik Deutschland Bundesdatenschutzgesetz a.F. (Expired on May 25, 2018 due to the law of June 30, 2017 (Federal Law Gazette I p. 2097) § 3a) in *https://dejure.org/gesetze/BDSG_a.F./3a.html.*

[29] Article 6 of GDPR states that: the processing is lawfulness if: *(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (b) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks. 2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX. 3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: (a) Union law; or (b) Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific. 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been*

In particular, in the case of the processing of data that are necessary for the operation of the vehicle, consent does not need to be collected, because the legal basis of the processing falls under art. 6, let. b., as necessary for the performance of the contract.

In case the processing for a purpose other than that for which the personal data have been collected is not based on the consent of data subject, according to the article 6, par. 4,

the controller have to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected. Precisely the controller shall to take into account: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Moreover, there is the case in which the data are collected, also in automated form, for the development of technologies similar to those purchased and used by the data subjects.

For example, through big data systems, such data could be collected to develop further technologies. In this case, depending on whether the requirements of art. 6, par. 4, you may need to seek consent to collect additional data unrelated to the purpose of the contract.

In other cases, when the purpose is completely unrelated to the purpose for which they were collected (e.g. for marketing purposes or for advertising), the consent of the data subject needs to be collected[30].

As well as when sensitive data are processed, IE those indicated in art. 9[31]. This even when

---

collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

[30] On the point see: L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali', (2017) II *Politica del diritto* 363 ff.; MC Gaeta, 'La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi' (2018) 1 Dir. inf. e informatica, 147 ff.; MC Gaeta, 'The issue of data protection in the Internet of Things with particular regard to self-driving cars' (2017) DIMT 1 ff.; IA Caggiano, 'Il consenso al trattamento dei dati personali' (2017) *DIMT online* 12 ff; L Aulino 'Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come rimedio ex ante' (2020) II *Diritto dell'informazione e dell'informatica* 303,312.

[31] Art. 9 of GDPR - Processing of special categories of personal data: "*1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. 2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be*

it is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 9 let. j of GDPR.

As recently outlined by the EDPB in its opinion 5/2019[32] on the interplay between the "ePrivacy" directive and the GDPR,13 art. 5,3 ePrivacy directive provides a rule that shall take precedence over art. 6 GDPR, with regards to the activity of storing or gaining access to those information already stored in the terminal equipment of a subscriber or user. In fact, this article states that prior consent is required for the storing of information, or the gaining of access to this class of information.

However, we can say that the personal data obtained by accessing information in the terminal equipment, must additionally have a legal basis under art. 6 GDPR in order to be lawful.

Since the controller has a duty to inform the data subject about all the purposes of the processing when seeking consent for the storing or gaining of access to information pursuant to art. 5,3 ePrivacy directive, the consent will normally also cover such processing operations.

Because of that, consent gained will likely constitute the legal basis both for the storing and gaining of access to information already stored and the processing of personal data following the aforementioned processing operations.

So, as we can see, the data processing as a whole involves specific activities for which the Eu legislature has sought to provide additional protection. That's why controllers must take into account the impact on data subjects' rights when identifying the appropriate lawful basis between the GDPR and the ePrivacy directive, in order to respect the principle of fairness. And there is a bottom line: art. 6 GDPR cannot be relied upon by controllers in order to lower the additional (and better) protection provided by art. 5,3 ePrivacy directive.

The EDPB recalls that the ePrivacy directive shares the same notion of consent as described in the GDPR and must meet all the requirements of the consent as provided by art. 4,11 and 7 GDPR.

However, art. 5,3 ePrivacy directive allows the processing of information that is already stored in the terminal equipment to be exempted from the requirement of informed consent, but only if it satisfy one of the following criteria:

- Exemption 1: for the sole purpose of carrying out the transmission of a communication over an electronic communication network;

---

proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. (j) ***processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*** *in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. 3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies. 4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health".*

[32] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, in *https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.*

- Exemption 2: when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

In such cases, the processing of personal data, those data already stored in the terminal equipment, falls under art. 6 GDPR's provisions.

Therefore, it may be considered unnecessary to collect the consent of data subjects only in certain specific cases, although it is more appropriate to collect consent.

4. Data processing in AutoMate.

In the AutoMate project, as described in chapter 2, a so-called AutoMate was developed to support the driver in special situations. For the present scientific work, a use case was used to investigate the extent to which case law is applicable to the Automate Assistant.

Since data protection and the use of data are at the center of this, this chapter must first clarify which data is used and how it is processed.

In the given example, the Protagonist Peter is driving the Car and could be supported by the AutoMate. To show Peter the HMI in Figure 1, the automation system acquires certain sensor values. These values can be subdivided in three categories: *Environmental data*, *explicit user data* and *implicit user data*.

Environmental data includes all data collected by the sensor system in the environment - independently of the driver in the environment. This includes e.g. the car coming from the front, the truck or the driven speeds.

In addition, *implicit user data* are also recorded for the application under consideration. These are for example information about the use of the system itself but also conclusions about the driving behaviour.

Explicit user data such as eye positions, tracking of emotions etc. are not yet recorded. However, these are under strong discussion for future applications.

Sensor data necessary for the AutoMate is stored in a temporary buffer after use for the HMI. For the model of the AutoMate, data in the model is processed anonymously so that the model changes. In this case, however, it is not possible to speak of a classic persistence of data, since the data is not written to a database[33].

Conclusions.

Given that the data used in the AutoMate experiment were completely anonymous and not attributable in any way, neither directly nor indirectly to a natural person, then the GDPR does not apply.

Consequently, there is no need to release the privacy information or collect consent to data processing.

If in the future data will be collected in any form that can be considered personal, according to the definitions of the GDPR, then it has to consider all the assessments that have been reported in the previous paragraphs to ensure compliance with processing in accordance with the GDPR.

Secondly, this study showed the importance of a multidisciplinary approach in the autonomous driving design that combines law, design and technology. Infact, incorporating legal regulations into the design phase can improve their ex ante application.

Furthermore, in this matter, it emerges the importance of introducing a code of conduct that can improve the application in every process of the principle of privacy by design and by default, ensuring adequate protection for the rights and freedoms of the data subjects

[33] M Eilers - E Fathiazar – Suck – T Stefan - D Twumasi, 'Dynamic Bayesian networks for driver-intention recognition based on the traffic situation' in *Cooperative Intelligent Transport Systems: Towards high-level automated driving* (Transport, IET Digital Library 2019), 465,495.

right from the design phase of the vehicle processing and construction.

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Autonomous driving: an exploratory investigation on public perception

ANNA IRENE CESARANO
Ph.D. Candidate in "Humanities and technologies" at University Suor Orsola Benincasa of Naples

Abstract

The automotive sector is constantly evolving, self driving cars are the result of a complex design that adopts a good variety of devices and sensors that capture information from the external environment which is then transmitted to an internal computer, in order to guarantee the vehicle efficiency, safety, stability. This text aims to present itself as an overview of the world of self-driving cars, glancing at my research project and focusing attention on the quantitative research conducted by me to test the level of knowledge of concepts such as robotaxis, automation, autonomous driving.

Keywords: Autonomous driving - Automotive sector - Research project - Public perception - Exploratory investigation - Automation - Robotaxis - Research design.

Summary: 1. The automotive sector. – 2. Autonomous driving as a benefical application of AI. – 3. Research project. – 4. The public's perception of autonomous driving. – Conclusions. – 5. ADAS: the project of a new investigation.

1. The automotive sector.

The automotive sector is constantly evolving. Self-driving cars are the result of a complex design that adopts a good variety of devices and sensors[1] that collect information from the external environment and then transmitted to an internal computer, in order to guarantee the vehicle efficiency, safety, stability[2]. In accordance with the meaning that we find in the most common dictionaries (eg Treccani), the term autonomous refers to the ability and the faculty to govern or stand up for oneself. The National Highway Traffic Safety Administration (NHTSA), or the US government agency for road safety, outlines a rather precise definition of autonomous car, noting that it is "a vehicle whose operation occurs without direct intervention by the driver to control steering, acceleration and braking and that it is designed in such a way that he does not expect to constantly check the road when the automatic mode is running[3]. In accordance with the above, it would be the vehicle's ability to detect external information with techniques such as Radar, Lidar, Gps etc., in a hybridization between these components and the advanced control systems on board the car, to allow the achievement of a certain degree of autonomy regarding the paths to follow and any obstacles and signals to be monitored.

[1] AI Cesarano, 'Empirical methodologies for the design of innovative autonomous driving solutions' (2020) EJPLT European Journal of Privacy Law & Technologies Giappichelli editore Issue 2020/1- 2020. http://www.ejplt.tatodpr.eu/Article/Archive/index_html?ida=190&idn=6&idi=-1&idu=-1

[2] AI Cesarano, *Autonomous driving: un'indagine esplorativa sulla percezione pubblica* Between science & Society Italian Institute for the future 2020.

[3] BC Zanchin, R Adamshuk, MM.Santos, KS Collazos, 'On the instrumentation and classification of autonomous cars', IEEE International Conference on Systems, Man, and Cybernetics, novembre 2017.

2. Autonomous driving as a beneficial application of AI.

Autonomous driving is a fruitful application of Artificial Intelligence (AI) in the automotive sector, which represents the future of smart mobility and whose applications will affect, as well as the automotive sphere, various aspects, not secondary, of the society in which we live. Today, AI can be found in the most diverse fields, from manufacturing to finance, from the healthcare sector to digital marketing, becoming the protagonist in what concerns the design, development, production and marketing of vehicles. AI is today at the center of a heated intellectual debate that sees scholars of different scientific vocations divided between statements and categorisations.

An univocal categorization of AI is somewhat difficult to propose precisely because it is a discipline straddling two scientific sectors, placing itself on two sides: that of a clear engineering matrix, which aims to build auxiliary machines for human activities and in some cases able to compete with Man in mainly intellectual tasks, e that of a psychological nature, oriented to build machines whose goal is the reproduction of the essential characteristics of human cognitive activity, arousing attention to some traditional philosophy diatribes and puzzles of the mind, for example the much debated mind-body problem[4]. In June 1956 four American scholars - John McCarthy, Nathaniel Rochester, Marvin Minsky and Claude Shannon - in an organized seminar in the United States (Dartmouth New Hampshire) it has remained historic for the definition of this discipline, laid the foundations of what would have been defined the programmatic basis of AI, defining the related research areas and the first programs for so-called "intelligent" computers. In the presentation the conference that marked the birth of AI reads:

In principle [by AI means] every aspect of learning and intelligence which can be described with such precision that it can be simulated with specially built machines. We will try to build machines capable of using language, to form abstractions and concepts, to improve themselves and solve problems which are still the exclusive domain of human beings[5].

The machines described by AI pioneers as "intelligent" are calculators digital, which by virtue of their particular characteristics and properties fundamental can be considered instruments with extraordinary symbolic processing skills, never seen before in a machine, and for this reason combined with some specific traits intrinsic to human intelligence. One of the most anticipated challenges of AI for the future, therefore, is represented by a "driverless" vehicle, as Elon Musk[6] said in 2016, founder of Tesla, one of the leading international giants in development of autonomous driving, in an interview with the BBC: "In the long term, nobody will buy a car unless it's autonomous. Owning a car that is not self-driving in the long term will be like owning a horse - you would own it and use it for sentimental reasons but not for daily use. The proliferation of research, studies and projects in the transport and logistics sector in the recent years is an indicator of the importance assumed by this particular strand of studies; in front of the numbers, there is no denying the great advantage that autonomous driving could offer to a technologically advanced society like ours. Every year in the worldwide there are about 1,400,000 people who die in accidents

[4] R Cordeschi, G Tamburini, 'L'Intelligenza Artificiale: la storia e le idee', in E Burattini, R Cordeschi, *Intelligenza artificiale. Manuale per le scienze umane*, Carocci, Roma, 2001.
[5] J McCarthy, M L Minsky, N Rochester, C Shannon, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence', August 31, 1955, AI Magazine, vol. 27 n. 4, 2006.
[6] C J Rory, 'Tesla chief Elon Musk says Apple is making an electric car', BBC News**,** 11 gennaio 2016

road, an authentic massacre. But the most accredited statistics speak clearly in relation the causes of these accidents, which in 90% of cases [7] (European Parliament, 2019) are attributable to inappropriate behavior or distraction of the driver; is only in one, to say the least, a small percentage, equal to about 2% of cases, liability it is attributed to technological defects in the vehicle (which, for the most part, depend on it from inadequate maintenance). As Butti[8] writes:

With the widespread diffusion of the driverless, the decrease in the number and the accident severity will be drastic: this is indicated by all forecasts independent scientific studies currently available […]. The benefits summarized above illustrated in terms of security are however sufficient by themselves to promote driverless driving technology.

3. Research project.

My research project is part of the "Research strategy and innovation for the intelligent specialization RIS3 Campania "and the areas of development in it: aerospace, cultural heritage, tourism, sustainable construction, biotechnology, human health, agri-food, energy and the environment, advanced materials and nanotechnology, transport and logistics[9]. The research involves the development of innovative systems to support autonomous driving (partially autonomous driving), combining one of the transversal sectors (Information & Communication Technologies) with a vertical sector (Transport and Logistics) of particular relevance for the Campania Region. In particular, the research theme involves the development of a new paradigm of safer and smarter mobility, with increasing automation quotas which must be harmonized with the characteristics of the human being to allow him to maintain an active role in the new socio-technical system. The research theme intends to investigate the methodologies necessary for the conceptualization, prototyping and verification of more suitable user interfaces to ensure effective interaction with the driver (in the context of partially or totally autonomous driving), taking into account technological aspects such as those relating to the individual and his cognitive, behavioral, etc. The application of innovative design methodologies (based on UCD and UX) will guide the design in the conceptualization phase, to allow a preliminary prototyping of the technological construct and its interface before it becomes a definitive product and allow to verify in advance how the people interact with the technological system. If this cooperation, studied through empirical methodologies, gives promising signals or highlights some critical elements, the user interface may be modified accordingly. Therefore, in addition to the conceptualization and prototyping methodologies, the development of technology verification methods are also an essential part of the innovative research system. Simulation environments are available within the Scienza Nuova[10] research center, both aimed at the automotive domain, and reconfigurable thanks to the presence of a driving simulator and a virtual environment in which different interaction experiences can be reproduced. Several technologically advanced tools can be used such as eye-tracking, biometric sensors, systems for detecting the emotional state through videocameras etc.

---

[7] https://www.europarl.europa.eu/news/it/headlines/society/20190410STO36615/le-statistiche-sugli-incidenti-stradali-mortali-nell-ue-infografica; Parlamento europeo, 'Le statistiche sugli incidenti stradali mortali nell'UE', 16 aprile 2019.

[8] L Butti, 'Auto a guida autonoma: sviluppo tecnologico, aspetti legali ed etici, impatto ambientale', Rivista giuridica dell'ambiente, n. 3/4, 2016

[9] http://burc.regione.campania.it

[10] The Scienza Nuova research center of the Suor Orsola Benincasa University of Naples is directed by professor Roberto Montanari, my tutor, who covers the teachings of cognitive ergonomics, interaction design, technologies for cultural heritage. Co-founder and R&D director of RE: Lab www.re-lab.it

4. The public's perception of autonomous driving.

However, the line of studies attributable to autonomous driving remains a niche sector confined to a limited audience and for the most specialist who really knows its functions and applications. For such reason, the goal of the research was to investigate and study perception and representation of autonomous driving in all its aspects, testing the level of knowledge of concepts such as automation, self-driving cars, robotaxis, to understand how much citizens really know about autonomous driving, touching topics like the security, trust[11], innovation, reliability, stability. The tab. 1 summarizes the research design, while in tab. 2 the conceptual map reports the indicators and dimensions explored by the study. The sample is formed by adults (18-65 years old) residing in Campania stratified by age, while the questionnaire is structured with closed questions, including some at the end relevant questions the "Other" option, where the interviewed can freely choose to write their answer on the question submitted. The territorial area is limited to the Campania provinces as Campania is the region where the doctoral project with an industrial character resides and is a particular topic relevant for this territory as already stated above[12], therefore the target of the research includes adults from Campania. The method used is the Web Survey through structured questionnaire, as it is impossible to conduct a study today without the aid of digital technologies that facilitate dissemination, collection, analysis and the identification of the target, which in this case also widely includes the so-called "digital natives"[13].

Research design

Tab. 1 Research design "Autonomous driving"

Research Questions:	Study the perception and representation of autonomous driving
Metodo:	Web survey
analysis unit:	Adults aged 18-65 years
Territorial area:	Campania provinces
Sampling:	Sampling reasoned choice
Population:	The set of adults aged between 18-65 residing in Campania
Data collection:	through a structured questionnaire

The dimensions explored by the study are socio-graphic, cognitive of the phenomenon and finally that relating to values, attitudes, opinions, representations of the concept. For each dimension it was considered useful to study some indicators: in particular for that socio-graphic age, gender, residence, educational qualification and employment status; in the cognitive dimension one is chosen to operate towards some indicators such as the level of knowledge of the sector, acquisition of the concept of autonomous driving, automation, robotaxis; the value sphere is widely investigated by numerous indicators such as perception

[11] The issue of trust in people is crucial for the introduction of self-driving cars, and the fear associated with a lack of security and stability cf. European Journal of Privacy Law & Technologies.

[12] Cf. http://burc.regione.campania.it

[13] M Prensky, 'Digital Natives, Digital Immigrants', On the Horizon, vol. 9 n. 5, ottobre 2001 (MCB University Press); A I Cesarano, *I nativi digitali tra rischi e opportunità. Le ricerche di EU Kids online,* Youcanprint, 2018.

topics related to autonomous driving through mass media and new media, mental (internal) representation of the subject, evaluation of opinions on autonomous driving (safety, utility, progress), perception and representation of the automation concept etc. The questionnaire is structured with 21 questions that they start from a generic theme, inherent to the research question about the means used for ordinary journeys, the time taken for such journeys, the system of public transport and the use of the car, to then go into the heart of the research by exploring with targeted questions the knowledge and perception of the

self-driving, of the robotaxi, and investigating in two specific questions legal and ethical issues related to civil liability in the event of a road accident.

Study the perception and representation of autonompus driving

Socio-graphic dimension	***Cognitive dimension of the phenomenon***	***Values,attitudes, opinions, representations, concept images***
Age	*Degree of knowledge of the sector*	*Perception of topics related to autonomous driving through mass media and new media*
Gender	*Acquisition of the concept of autonomous driving*	*Representation of the internal concept (mental image of the subject)*
Residence	*Personal knowledge of autonomous driving concept vs. actual concept*	*Representation of the external concept (image that external subjects give)*
Educational qualification	*Knowledge of the concept of automation*	*Evaluation of opinions on the autonomous driving (safety, utility, progress etc.)*
Employment status	*Knowledge of the concept of robotaxis*	*Degree of differentiation between opinions and the autonomous driving sector*
		Opinions about the autonomous driving
		Perception and representation of the concept of automation
		Perception and representation of the concept autonomous driving
		Perception and representation of the concept by robotaxi

Tab. 2 - Conceptual map of indicators and research dimensions

The fifth question of the survey was intended to analyze both the cognitive dimension of the phenomenon that the value[14]: the user is asked through a frequency scale that goes from "never" to "very often" if in the last six months, through the mass media and new media, had had knowledge of the self-driving. What clearly emerges from the data is that the "never" dominates the others answer options, such as questions "read a newspaper article" or "seen an online video of a car driving alone" (fig. 1).



Fig. 1 Frequency with which in the past six months respondents have come into contact with the concept of autonomous driving.

So there is very little knowledge of the concept of autonomous driving, even if the sample was made up of a percentage of very young people who it stands at around 40% (equal to about 112 people out of 235 in total) of the sample with an age ranging from 18 to 35 years, with a strong familiarity with the new technologies. The "no" (64.8% of cases) is also the answer with the highest percentage to the question "Have you ever driven a car equipped with assistance systems to guide?" (Fig.2)

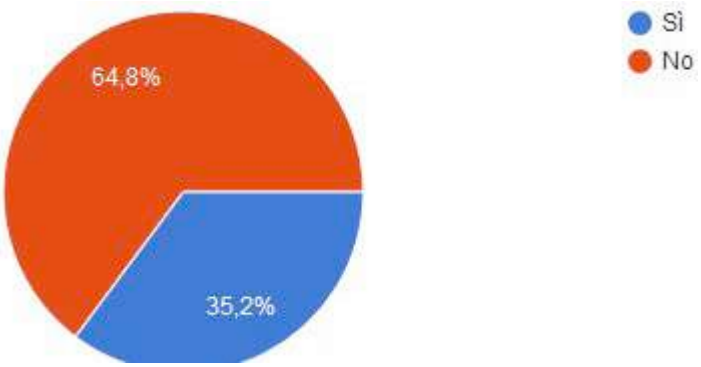


Fig. 2 Answers to the question: "Have you ever driven a car equipped with driver assistance systems?"

However, factors emerge in subsequent responses to the questionnaire important worthy of consideration. Despite little or no knowledge autonomous driving (predictably) by a considerable share of the sample, which by the way was composed mostly of women (about

[14] In table 2 it is possible to consult all the dimensions, including also the cognitive of the phenomenon and values.

64.8%) which could be considered as a "gender gap" in that less interested in this sector and less informed on this, it does not emerge from the data a complete mistrust in the safety of autonomous driving, as we might expect. This is clear from the answers to the question of whether with the introduction of the robotaxi could increase road accidents: only one person replied "10" (very likely) on a scale of 1 to 10 (235 replies total) while the highest frequency was 1, as can be seen in figs. 3-4, but a certain condition of uncertainty about the real possibilities offered by autonomous driving dictated by a poor knowledge of the sector. Consequently, it is logical think that if people had a greater perception and knowledge of autonomous driving, they would have greater confidence and less fear at the introduction driverless cars.

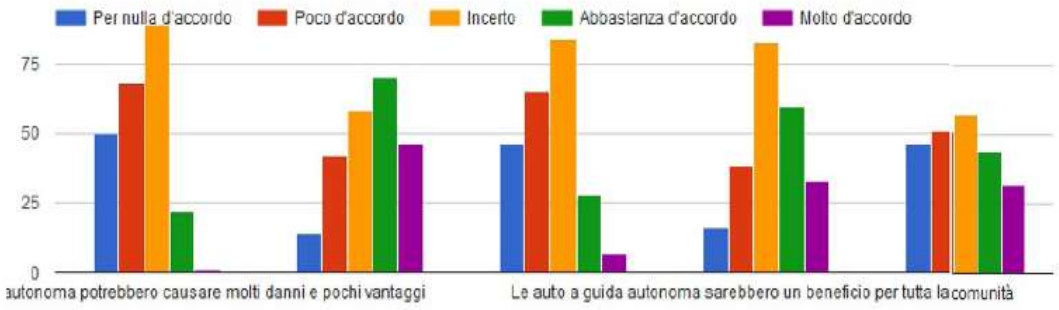


Fig. 3 Perception of the risks and benefits associated with autonomous driving

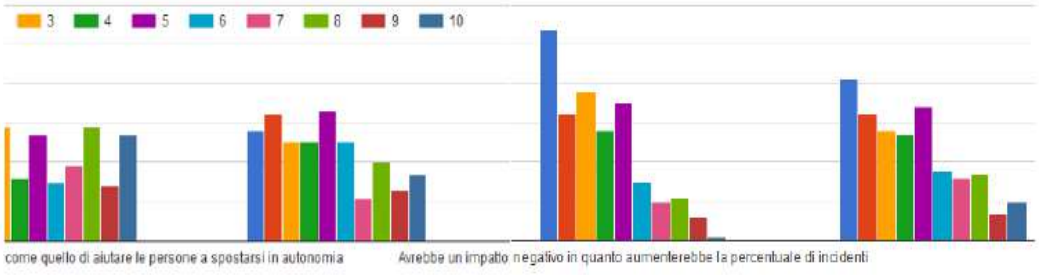


Fig. 4 Perception of the risks and benefits associated with autonomous driving, in particular the introduction of Robotaxis.

The condition of uncertainty is clearly visible from the data: in fig. 3 the frequency higher is almost always around "uncertain", even when it is exceeded by little to "agree enough" to the statement whether self-driving cars represent a desirable progress. This confirms the above, or that people have no mistrust of autonomous driving, but they do not have a correct knowledge, a correct perception and above all they do not feel informed on this matter, but still show that they have an interest in this sector and consider it a technological advance, so they have an internal mental image of progress. In the diagram in fig. 5 it is possible to note that 48.7% of users responded with an image of progress and technological advancement to the question “What representation comes to your mind of reading the definition of autonomous driving? ".



Fig. 5 Answers to the question "What representation comes to your mind when reading the definition of autonomous driving?"

The ethical-legal issue seems to be one of the most critical, if not the most critical thorny, for the introduction of self-driving cars. The principle of responsibility civil and criminal in road accidents turns out to be a theme of heated debates and able to channel the attention of several scholars[15]. Within the research, this thorny problem is addressed in two questions, asking users directly for their opinion in case of road accident both with a fully autonomous car and with a partially autonomous car. From the two pie charts in fig. 6-7 a tangible difference immediately emerges in the responses of users to vary (albeit slightly in drafting and reading, but which however has a great meaning) of the question asked. In a car a fully autonomous driving, according to the sample subjects the responsibility civil and criminal would be in 27.8% of the cases of the company that manufactures the car (manufacturer), while in 24.8% of cases it would fall on the company that produces the car components[16] (manufacturer of the product components), and in 22.6% of the cases is the company that produces the self-driving car components that the owner of the car; the remaining percentages are divided between the owner of the car (17.4%) and very low shares that stand at around 0.4% (equal to 1 person), for different answers given freely through the option "Other" contemplated at the end. In a partially self-driving car it stands out instead a rather high percentage, equal to 39.1% of the answers, which he attributes responsibility to the owner of the car, while a 34.8% is to the owner of the car that to the company that produces the product components; the remaining percentages are divided into 11.7% for the company that produces the components of the car, 7.8% for the company that produces the car and shares equal to 0.4% for every person who has given free answer to this question.



[15] For a complete and somewhat exhaustive discussion on the subject, see M C Gaeta, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies* (ESI 2019)
[16] Sensors, videocameras, etc.

Fig. 6 Answers to the question "In a hypothetical accident committed by a fully driven car autonomous, whose civil and criminal liability would it be?"



Fig. 7 Answers to the question: "In a hypothetical accident committed by a partially driven car autonomous, whose civil and criminal liability would it be?

Conclusions.

From a comparison between the answers to these last two questions one could affirm that in the case of totally autonomous driving, people attribute the responsibility of the road accident to subjects who do not identify themselves in car owner, but who seem rather divided between various subjectivities external, e.g. the company that manufactures the car, or the components of the car, or in concomitance with the owner. Otherwise it happens when the car is driving partially autonomous: in this case the responsibility is recognized both in the subjectivity of the car owner (39,1%) both when the latter is in concomitance with the company which produces the autonomous driving components(34,8%). Finally, as far as the concept of automation is concerned (fig. 8), it seems re-propose that condition of uncertainty and neutrality that occurred in some questions on the effects of autonomous driving. In fact, most responses on a frequency scale of 0 to 10 stand at around 5, featuring a condition of indecision, perhaps due to lack of elements to express oneself,

but the aforementioned people's consensus on technology and progress is proposed again: to statements such as "the automation of everyday life I it perplexes "or" I find it aberrant to replace machines with beings humans ", the highest frequency is 0.

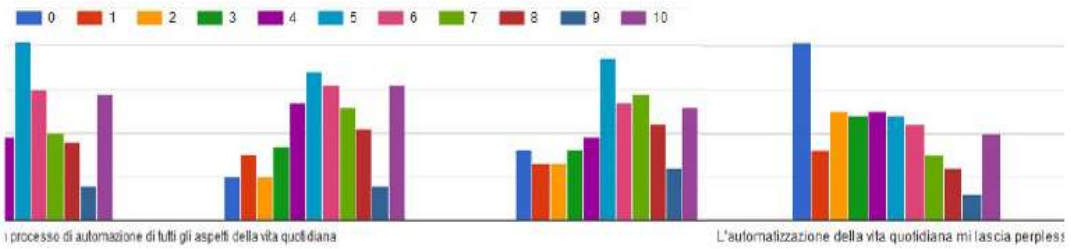


Fig. 8 Perception of risks and benefits to the automation of daily life

5. ADAS: the project of a new investigation

The project of the new survey will focus on advanced driver-assistence systems (ADAS), the goal is to investigate and study the perception of accidents and near misses through the systems called ADAS, structured into two sections, one concerning the knowledge of the

functioning of the system, the other focused on accidents and near accidents. The tab. 1 summarizes the hypothesis of the research design developed, not yet implemented but in the testing phase, in fact at the present time the questionnaire structured through Google modules has been sent to a first panel of experts both in ADAS and in methodologies, i.e. those who have ADAS domain competence or technical competence on the construction of the questionnaire and on the analyzes, to collect the first comments and suggestions in view of the final version to be disseminated both in Italy and in Sweden. The pilot study within the RE: Lab of Reggio Emilia[17] is conducted on a small selected sample of people to analyze some categories of the research that will eventually undergo changes, after the conclusion of this survey to refine some questions. Given the experimental nature of the study, it is not possible to define in this phase the unit of analysis and the population to which the survey is addressed, i.e. the subjects and the set of target subjects of the research, as it will be decided in one phase implementation of the users to be involved in the study. The questionnaire is

structured with 28 closed questions, and is divided into several sections. In the first part, the research objective is to investigate the knowledge of the functioning of the system by focusing attention on the various ADAS, and in some questions to test people's real knowledge of Adaptive Cruise Control and of the difference in operation with another ADAS the Cruise control. In the second part, the research objective is aimed at investigating the perception of accidents and "near accidents" near accidents in relation to use and interaction with ADAS, the responsibility of ADAS in road accidents and near road accidents. The method used is the Web Survey as it is impossible today to conduct a study without the aid of digital technologies, that facilitate the dissemination, collection, analysis and identification of the survey target.

Table 1 Hypothesis of research design ADAS advanced driver-assistence systems

Research Questions:	Study the perception of accidents and near misses through ADAS
Metodo:	Web survey
analysis unit:	
Territorial area:	Italy
Sampling:	Sampling reasoned choice
Population:	
Data collection:	through a structured questionnaire

[17] Roberto Montanari, my tutor, who covers the teachings of cognitive ergonomics, interaction design, technologies for cultural heritage. Co-founder and R&D director of RE: Lab www.re-lab.it

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Human machine interaction and legal information in the autonomous vehicles: the opportunity of the legal design

LIVIA AULINO
Ph.D. Candidate at the University of Naples Suor Orsola Benincasa
Lawyer

Abstract

The paper deals with the relationship between language and law and then examines the connection between autonomous driving and law. Therefore, the fundamental question includes both what are the best ways of transmitting legal information within autonomous vehicles as well as their correct understanding.

The issue of the lack of clarity of information from the private law point of view will then be addressed, focusing on the issue of error in view of an evolution of the category.

In this context it is considerable of the role of design and in particular of legal design, as a possible remedy to the communication deficit of legal information provided by the vehicle. In fact the solution can be seen in the opportunity to design human machine interfaces, which - also through an acoustic signaling, visual or tactile - provide clearly and unambiguously legal information on the autonomous vehicle. This in order to guarantee a security by design and to ensure support and mutual learning between the machine and the user.

Keywords: Automation - Autonomous vehicles - Human Machine Interaction - Legal information - Law by design - Legal design - Methodology - Interdisciplinary research.

Summary: Introduction. – 1. Autonomous driving as a multimedia habitat. – 2. The relationship between language and law. – 2.1. Legal information in autonomous vehicles. – 3. Data protection issues. – 4. Another example of potentially missing information: Adaptive Cruise Control and Child Presence detection. – 5. The lack of clarity of the information from a private law point of view: linguistic error vs obstacle/defective error in view of the evolution of the category. – 6. Hypothesis of solution in the design: the legal design methodology. – Conclusions.

Introduction.

The development of the new Internet Of Things (IOT) and Artificial Intelligence (AI) technologies will have a strong impact especially in the automotive field. In fact, the car of the future will consist of four essential elements: connection, electricity, autonomy and sharing[1].

In particular for the realization of autonomous driving it will be necessary to adopt technologies of connection V2X[2]. Vehicles will be equipped with high-performance communication systems to allow a continuous exchange of data between vehicles, roadside infrastructure and pedestrians. This level of connection will increase the ability to perceive

[1] 'Smart & Connected Car: un mercato da 1,2 miliardi' (2020), available on *https://www.osservatori.net/it/ricerche/comunicati-stampa/smart-connected-car-un-mercato-da-1-2-miliardi.*

[2] V2X (*Vehicle-to-everything*) is a system of communication of information between a vehicle to any entity that can influence the vehicle and vice versa.

the environment and coordinate manoeuvres in complex scenarios. All this should translate into safer, sustainable and efficient mobility.

Vehicles will be smarter and more autonomous, as will be seen below, but also shared. In fact, new forms of car sharing will develop.

This question requires a necessary reflection on the legal aspects that will characterise the automotive field.

1. Autonomous driving as a multimedia habitat.

Recently, automation is rapidly developing, and becoming a constant in everyday life, therefore it is no longer a question of a remote and future possibility but of a concrete reality.

In particular, technological development is producing remarkable results in the automotive field where new technologies have enabled vehicles to be equipped with useful systems to facilitate machine control and to support driver activities.

An autonomous vehicle (AV) is capable of moving safely with partial or no human help thanks to a complex system of sensors, software, etc. For this, the autonomous vehicle could be referred to as a multimedia habitat. All these components of the autonomous vehicles are capable of processing a huge amount of data in order to use them through the different multimedia systems characterizing the concept of the AV. That is enough to include AV in the concept of "multimedia habitat".

ADAS[3] (Advanced Driver Assistance Systems) do not take control of the vehicle but they merely assist the person who is driving at that time.

In 2019, the European Parliament adopted a Legislative Resolution on the proposal for a Regulation of the European Parliament and of the Council which established that in Europe will be mandatory the adoption of ADAS systems in vehicles to protect passengers, pedestrians and cyclists[4].This will also have real safety benefits.

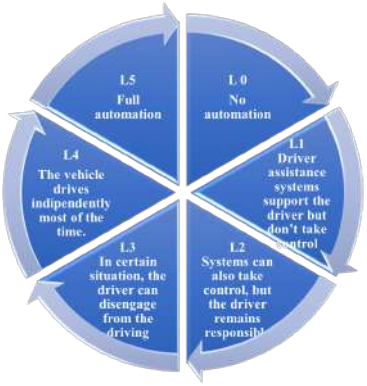
The European Parliament has confirmed that most of these systems will have to be adopted by all new approval models introduced on the market from May 2022. The new equipment will become mandatory from May 2024 for all the cars that are already on the market.

As regards autonomous driving, in 2014, SAE International (Society of Automotive Engineers) published an international standard that defined six different levels for

[3] ADAS are driving aid systems with effects on the driving choices of individual vehicles (driving behaviour) or vehicle sets. They are generally oriented to safety (active and preventive) and driver comfort. ADAS systems improve road safety by reducing the number of accidents and have an immediate indirect effect on the condition of the vehicle currents. On the point: *http://www.mit.gov.it/mit/mop_all.php?p_id=17684*.

[4] The mandatory ADAS (Advanced Driver Assistance System) will be: adaptive speed control; driver fatigue detection; engine start; adaptive speed control; driver fatigue detection; engine start after breathalyzer; automatic emergency braking; black box; running lane maintenance; collision avoidance with pedestrians and cyclists; distance detection; tyre pressure monitoring.
A study of SBD Automotive has found that in 2025 the European market of the ADAS will grow 70% and will be worth approximately 3,71 billion euros. To deepen: *https://www.ilsole24ore.com/art/nel-2025-mercato-europeo-adas-varra-371-miliardi-euro-ACpjm0K*

autonomous driving[5]. The classification is based on how much the driver has to take action, rather than on the capabilities of the vehicle.



Level 0: a traditional car with the exception of automatic emergency braking, which blocks the car when the sensors detect an obstacle in front of the vehicle.

Level 1 (Driver Assistance): the vehicle features a single automated system for driver assistance, such as steering or accelerating (cruise control).

Level 2 (Partial Driving Automation): the vehicle can control both steering and accelerating/decelerating. Here the automation falls short of self-driving because a human sits in the driver's seat and can take control of the car at any time.

Level 3 (Conditional Driving Automation): vehicles have "environmental detection" capabilities and can make informed decisions for themselves, such as accelerating past a slow-moving vehicle. But they still require human override.

Level 4 (High Driving Automation): these cars do not require human interaction in most circumstances. However, a human still has the option to manually override. Level 4 vehicles can operate in self-driving mode. Anyway, until legislation and infrastructure evolves, they can only use them within a limited area.

Level 5 (Full Driving Automation): vehicles do not require human attention. Level 5 cars won't even have steering wheels or acceleration/braking pedals. They will be free from geofencing, able to go everywhere and do everything that an experienced human driver can do.

Indeed, some international surveys highlighted that half of the participants showed distrust of autonomous driving and more than a third showed some anxiety. Concerns were mainly due to the fact that people do not trust the car enough to leave full control, especially in the emergency situations.

This means that the success of future automation systems will necessarily depend on the ability of manufacturers to create a solid human-machine team as well as on the quality of interaction, communication and cooperation, to achieve safety, efficiency and comfort. This cooperation has above all the purpose of increasing confidence in the multimedia habitat represented by humans and vehicles, to fully exploit the potential of automation to improve human life.

Accordingly, in the design of a complex socio-technical and high automation system such as the partial or total autonomous vehicle, an approach that places the human factor at the center cannot be ignored, particularly when it comes to its user interface design. In this context emerges the importance of the design focused on the human-machine relationship, as a suitable methodology to guarantee an effective human-machine cooperation.

2. The relationship between language and law.

What is the connection between autonomous driving and law? Law and automation both "work" with information. The law is a set of information, which need to be transmitted; in fact, legal studies have always revolved around the ways in which human beings process, share and use information[6].

Legal logic has always been a matter of study, but now more than a capacity for

[5] See *https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic.*
[6] R Caterina, *I fondamenti cognitivi del diritto* (Mondadori 2008) 1.

"persuasion" with good rhetoric, we need a strong logic to teach a robot[7].

The key issue is the best way of providing information and its correct understanding. Therefore, the solution requires that the conditions are created for these choices to be weighted, aware, informed.

This approach necessarily implies a close dialogue with the cognitive sciences and must be at the basis of the design of autonomous driving.

In support of the need for an interdisciplinary dialogue between law and the cognitive sciences, it should be considered that the jurist, who handles knowledge, decision or will problems on a daily basis, must decide whether the notions of common sense can be supplemented by the teachings of cognitive sciences.

The jurist who deals with informed consent cannot ignore some psychology issues such as factors that influence a decision[8]. Hence, the law must have a pragmatic approach, especially attentive to the way cognitive and decision-making processes are carried out.

This need to consider knowledge in the cognitive field is very clear, for example, in the field of consumer protection. Article 5, 3, consumer code[9], in fact, that provided the information to the consumer, must be communicated in a clear and understandable way, such as to ensure the awareness of the consumer, and also taking into account how the contract is concluded or the characteristics of the sector.

For this purpose, information requirements are introduced for undertakings. However, the question arises of how to modulate the content of these obligations, both in relation to the amount and quality of the information to be provided to the consumer, and in relation to the concrete ways of expression which must convey this information, considering the cognitive limitations that afflict the recipient of the communication.

The results of the psychology studies of the decision can be relevant in identifying the correct methods of communication of the information necessary to level asymmetries where consumers are in disadvantage compared to professionals.

Cognitive psychology has demonstrated the existence of a number of strategies that individuals employ in dealing with decisions. It whether such decisions are made in a state of uncertainty or lack of information[10], such if these are taken in environments whose information rate is so high that it puts in crisis the analytical skills of the individual[11].

Consequently, the law must necessarily study the cognitive structures of language and language itself, establishing a parallelism with the latter.

This assertion applies to all the words, spoken or written, of laws, judicial decisions, agreements between individuals, etc.

Thus, the problem of the law is fully identified with the problem of language[12].

The stability and continuity of the meanings that words take on gives rise to the trust of all the members of the linguistic community. Hence, the addressees of the legal provision

---

[7] C Morelli, 'Avvocato 4.0: un mare di buone letture' (2020) available on *https://www.altalex.com/documents/news/2020/08/03/avvocato-4-0-un-mare-di-buone-letture.*

[8] R Caterina, *I fondamenti cognitivi del diritto* (Mondadori 2008) 4.

[9] Article 5,3 of Legislative Decree, 6.09.2005, n. 206 (consumer code): "*Information to the consumer, from whomsoever it originates, must be adapted to the communication technique used and expressed in a clear and comprehensible way, also taking into account the modalities of conclusion of the contract or the characteristics of the sector, such as to ensure consumer awareness*".

[10] D Kahneman, P. Slovic, A Tversky, *Judgment Under Uncertainty: Heuristic and Biases*, (Cambridge University Press 1982).

[11] A Tversky, D Kahneman, 'Availability: A Heuristic for Judging Frequency and Probability' (1973) 5 Cognitive Psychology, 207,232; D Kahneman, A Tversky, 'Prospect Theory: An Analysis of decision Under Risk' (1979) 47 Econometria, 263,291; D Kahneman, JL Knetsch, RT Thaler, 'Experimental Test of the Endowment Effect and the Coase Theorem' (1990) 98 Journal of Political Economy, 1325,1348.

[12] N Irti, *Riconoscersi nella parola* (Il Mulino 2020) 81.

trust that the words used by the legislator are bearers of a firm content[13].

2.1 Legal information in autonomous vehicles.

From now on, the paper examines the question of the "information" that are provided to autonomous vehicles in order to enable them to function.

Connected and Autonomous Vehicles (CAVS) are capable of communicating and receiving data from the external environment, road infrastructure and other vehicles through the use of state-of-the-art cameras, sensors and technologies, and then rework them through a software that can replace the driver in the performance of part or total of certain driving functions[14].

It follows that, if at present models of cars equipped with assisted driving functions are available[15] allowing automatic management of manoeuvres such as parking, anti-lock braking systems or adaptive cruise control. It is now possible to imagine the next arrival of fully automated cars, in which the human driver, completely replaced by the on-board software, will be nothing more than a mere passenger, almost as if using a train or an airplane and this would be the third level of automation.

The driver - passenger continues to play a leading role. In fact despite such a level of automation, the driver has to maintain a constant and maximum alert status, even when the vehicle is being monitored by the on-board software. The driver has to resume immediately driving whenever he is instructed to do by the programme or if there are circumstances that require it[16].

In this case, it is necessary to exploit again the interdisciplinary approach that analyses the mechanisms, the causes, the effects of the phenomenon of "human error" to try to finally answer the question whether it is possible to circumscribe with certainty a legal regime of error.

To understand how liability is defined, it is noted that there is a strong correlation between the risk of a road accident and the error made by the driver of the vehicle[17].

A study was conducted in the USA in 2016[18] analysis and monitoring of road accidents that has ascertained how the behaviour of the driver contributes to the accident. The study found that out of 905 accidents during the observation period, 87.7% had at least one error, mostly due to certain situations:

- non-optimal state of the driver, compromise by effect of alcohol or drugs; tiredness, sleep stroke, emotional state (crying, anger, sadness, agitation). In particular, the non-optimal driver conditions increase the risk of an accident by 5 times. In the case of drunk driving, the risk would increase by 36 times more. The emotional state of

---

[13] Ibid 87-88.

[14] This refers to vehicles with V2X (vehicle-to-everything) connection technology, which incorporate V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) technologies partly already existing on the market and with varying application not only in the field of road traffic but also aeronautical and maritime.
For further information see: S Pellegatta, 'Autonomous Driving and Civil Liability: The Italian Perspective', (2019) Giureta - Riv. dir. econ. trasp. amb., 135 ff.; MC Gaeta, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies* (Editoriale Scientifica 2019).

[15] Driver assistance: functions involving partially or fully automated driving, such as operational assistance or autopilot in heavy traffic, in parking, or on highways. See: European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, adopted on 28 January 2020.

[16] R Lobianco, 'Veicoli a guida autonoma e responsabilità civile: regime attuale e prospettive di riforma' (2019) 3 Responsabilità Civile e Previdenza, 724.

[17] L Bensalah, 'Errare humanum est. L'errore nel diritto tra intenzionalità, razionalità, ed emozioni', (2018) 45 Trento Law and technology, Research Group Student Paper, 83,86.

[18] The study was conducted by the Virginia Tech Transportation Institute, "Dingus 2016". See: *https://www.internazionale.it/scienza/2016/02/27/incidenti-auto-motivi*

sadness or agitation increases the risk by about 10 times.
- Driver performance error.
- Temporary error of judgement (distances, timing, speed).
- Distraction (use of devices; interaction with passengers; external factors). The distraction of drivers would double the risk of accidents.

In Italy the subject is particularly important, so that two new crimes have recently been introduced in the context of road accidents. In fact, the L. n. 41/2016 introduced the article 589 *bis* of criminal code "Road murder" and article 590 of criminal code "Serious or very serious personal injury".

The European Commission in 2015 published a report aimed at suggesting to road safety professionals some good practices to reduce the risk of road accidents, considering the constant increase of the phenomenon of distraction and the commission of errors in the conduct of road vehicles.

Among the indications:
- wireless technologies and applications to reduce driver-device interaction;
- systems to limit distraction such as collision warning signals, lane departure warning, emergency brakes;
- educational and enforcement actions to monitor the application of existing laws;
- mobile phone call locking systems and advanced driver warning systems;
- drafting of common guidelines for the automotive and telecommunications industries with a view to defining standards for the installation of man-vehicle interface systems, of functions for the blocking of calls from mobile phones, of wireless devices on the dashboard of the car.

This, however, is a reasoning valid only up to the third level of automation. From the fourth level of automation, in fact, the driver would end up concretely losing his distinction from the simple passenger. Already at this stage the vehicle will be fully operated by the on-board software for the entire duration of the journey, without having to comply with the same obligations as in the case of a level 3 AV.

However, the scenario of the CAV level 4 calls for reflection. If with a level 3 CAV the information is provided to the pilot software and the driver must constantly remain on "alert", with a higher level CAV the human action should stop the entry of data, ie information, several of which have legal character, and to their transmission (including between autonomous vehicle and passenger-driver).

The fact that the legal information is not clear and immediate in its understanding contrasts with the need to guarantee a high degree of situation awareness in the operational framework of the user. In particular, inside the vehicle where the human machine interfaces provides legal information that communicates an obligation to be respected (and precisely on: privacy and data protection; shared control; support and mutual learning).



3. Data protection issues.

It is necessary to consider an aspect of the matter: the processing of data in autonomous driving and the awareness of the user on it.

On the point it was selected and analyzed an use case from the *AutoMate* project, in a separate paper. In particular, the use case was analyzed because it can be investigated to what extent and whether user data is collected and processed in autonomous driving[19].

Vehicle drivers and passengers may not always be adequately informed about the processing of data taking place in or through a connected vehicle.

It is not enough that the information is given only by the vehicle owner, who may not be the driver, and may also not be provided in a timely manner. Thus, there is a risk that there are insufficient functionalities or options offered to exercise the control necessary for affected individuals to avail themselves of their data protection and privacy rights.

This point is very important because during their lifetime, vehicles may belong to more than one owner either because they are sold or they are being leased rather than purchased. In addition, vehicles are increasingly being shared or rented, not just by companies, but also by individuals, and by the person whose data is collected, may not be able to object to some data processing[20].

There is both a lack of control and information asymmetry[21], but that is not the worst thing.

In Fact, the flow of data in and out the vehicle should also be triggered automatically as well as by default, without the individual being aware of it, avoiding his control on the data sharing functions of the CAV.

The consent about this flow of data should be collected.

When the data processing is based on consent, all elements of valid consent have to be met according to the GDPR[22], which means that consent shall be free, specific and

[19] L Aulino, M Saager, MC Harre, L Espindola, 'Consideration of privacy aspects in the area of highly automated driving. An intention recognition use case' *EJPLT* in course of publication.

[20] 'Connected Cars: What Happened to Our Data on Rental Cars' (2017) Privacy International, *https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf*

[21] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, (n. 15).

[22] Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) applicable as of May 25th, 2018 in all member states to harmonize data privacy laws across Europe.

informed[23] and constitutes an unambiguous indication of the data subject's wishes as interpreted in EDPB guidelines on consent[24].

For this reason, data controllers need to obtain valid consent from different participants, such as car owners or car users. Such consent must be provided separately, for specific purposes and may not be bundled with the contract to buy or lease a new car.

The same principles have to be applied when consent is required to comply with the "ePrivacy" directive, for example if there is a storing of information or the gaining of access to information already stored in the vehicle as required in certain cases by art. 5(3) of the "ePrivacy" directive.

It is necessary that CAV users (with no distinction between their owners and the "simple" users) are made aware of the data processing functions, of their purposes. In fact a similar unawareness constitutes a significant barrier to demonstrating valid consent under the GDPR, as the consent must be informed[25].

In such circumstances, consent cannot be relied upon as a legal basis for the corresponding data processing under the GDPR, unless the processing is necessary for the protection of the safety of data subjects (in this case, consent is not required according to article 6)[26].

It is needed to re-think the mechanism used to obtain consent, because the main one may be too difficult to apply in the context of connected vehicles, resulting in a "low-quality" consent based on a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals[27]. We can imagine, for example, the case of drivers and passengers who are not related to the vehicle's owner in the case of second-hand, leased, rented or borrowed vehicles.

In the absence of the possibility to effectively control how the vehicle and its connected equipment interact, it is bound to become extraordinarily difficult for the user to control the flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep.

It is important to consider one last thing: the data need adequate protection. In fact, The plurality of functionalities, services and interfaces offered by connected vehicles increases the attack surface and thus the number of potential vulnerabilities through which personal data could be compromised. Unlike most Internet of Things devices, connected vehicles are critical systems where a security breach may endanger the life of its users and people around.

It is thus heightened the importance of addressing the risk of hackers attempting to exploit vulnerabilities of connected vehicles.

Considering everything, the writer is working on a research to propose a privacy disclaimer to be installed inside autonomous vehicles that is designed according to law by design methodology.

---

[23] Art. 4 of the GDPR: "11. *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"

[24] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, (n. 15).

[25] L Aulino, M Saager, MC Harre, L Espindola, 'Consideration of privacy aspects in the area of highly automated driving. An intention recognition use case', in course of publication.

[26] Eg. *Ecall device*, mandatory from 2018. On the point: MC Gaeta, 'The issue of data protection in the Internet of Things with particular regard to self-driving cars' (2017) DIMT 1 ff.

[27] On the point see: L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali', (2017) II *Politica del diritto* 363 ff.; IA Caggiano, 'Il consenso al trattamento dei dati personali' (2017) *DIMT online* 12 ff; L Aulino 'Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come rimedio ex ante' (2020) II *Diritto dell'informazione e dell'informatica* 303,312.

In the case of resale of a connected vehicle, the ensuing change of ownership should also trigger the deletion of any personal data, which is no longer needed for the previous specified purposes. For this reason, it is reasonable that traditional mechanisms to obtain consent may be difficult to apply in the context of connected vehicles.

4. Other examples of potentially missing information: Adaptive Cruise Control and Child Presence detection.

Adaptive cruise-control[28] is an ADAS that uses a radar (or laser) sensor to monitor the distance from the vehicle that travels in front and, if this distance drops below the safety threshold, reduces the speed of the car. When the road is free again, the Adaptive cruise control automatically changes the speed to that set.

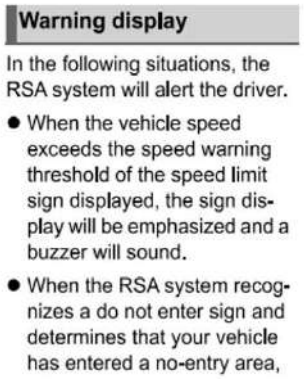
The question that arises is whether the ACC is set in the vehicle, which will then follow a predetermined cruising speed, but you are faced with a road sign that identifies a lower speed limit for that same road.

The question arises on how and whether the vehicle will inform the driver of the speed limit and whether there is a communication deficit in the provision of such legal information.

In fact in these cases the vehicle could either alert the driver with a warning light, inviting him to change the speed manually, or even better automatically adjust the speed to the limit provided for that road.

In order to verify the existence of communication limits in the provision of this information, a benchmarking study has been conducted[29], in which four vehicles were compared.

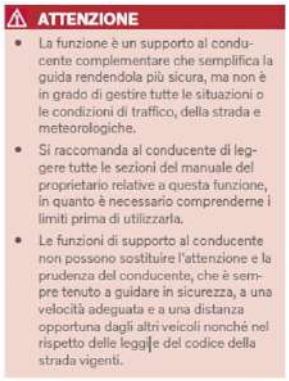
The analysis showed that in samples 1, 2 and 3, the vehicle, in case you find a different speed limit than that set by the ACC, will advise the driver - through a tell-tale - to change the speed with manual control.



Sample no. 1



Sample no. 2



Sample no. 3

In sample no. 4, the ACC maintains the set speed whenever no vehicle is detected in front of it. Otherwise it accelerates and decelerates according to the speed of the previous vehicle. Nothing says with reference to the speed limits.

---

[28] The ACC system was first introduced in 1995 by Mitsubishi, which installed it (with a laser sensor) on a car destined for the Japanese market. Subsequently in 1997 and 1998 it was developed in Europe by other car manufacturers. Since then, this technology has spread to numerous medium-high range models and in fact represents a fundamental step towards autonomous driving. To know more: *https://www.quattroruote.it/guide/Guida-assistita/cos-e-e-come-funziona-il-cruise-control.html*

[29] Benchmarking means a methodology based on systematic comparison that allows companies to compare themselves with the best and above all to learn from them (definition extracted from *https://it.wikipedia.org/wiki/Benchmark_(economia)*



Sample no. 4

Instead, from sample no. 5, it emerged that in case there is a different road speed limit from the one set by "*Active distance assist distronic*", then the new speed adapts autonomously. There is no need for driver intervention.



Sample no. 5

Nevertheless, it is clear that the driver must be properly informed about how the system works in order to use it consciously.

This, however, may not be enough to ensure its proper use, as will be seen in the next paragraph.

Another case study concerns the Child Presence detection [30]. Today, the main cause of deaths of children in cars is due to the fact that the driver, upon arrival at their destination, accidentally forgets them in the vehicle [31].

[30] L Aulino, 'La sicurezza dei minori in automobile nello sviluppo della guida assistita: dalla disattivazione air-bag al dispositivo anti-abbandono' (2019) *DIMT online*, 1,17.

[31] According to data collected by a researcher at San Jose State University (Null, 2014), in 2014, there were at least 30 deaths from heatstroke of children in cars. Null states that from 1998 to 2014, an average of 38 children are dead annually from automotive heat stroke in the United States. An NHTSA survey of non-road accidents in 2007 found that hyperthermia (heatstroke) was the third most common non-road vehicle death scenario for children under 14 (NHTSA, 2009).

Furthermore, the child's inability to get out of the vehicle alone combined with a low tolerance for high temperatures, can cause him to suffer from heat stroke, even if left alone for a few minutes in the car.

Law no. 117/2018 and the subsequent Decree of the Ministry of Transport of 02 october 2019 introduced the obligation for parents to equip themselves with Child Presence detection precisely to deal with this emergency.

These devices can be designed as ADAS inside the vehicle or as devices in child restraint systems or independently of both.

In particular, pursuant to article 3 of the Ministerial decree, the anti-abandonment device can be:

a) originally integrated into the child restraint system;

b) a basic equipment or accessory of the vehicle, included in the information package of the vehicle type-approval;

c) independent of both the child restraint system and the vehicle.

These regulatory data are accompanied by article 3.2 of the *assessment Protocol - Child Presence detection*, issued by Euro NCAP in September 2019[32], according to which it is possible to deactivate this driving assistance system both temporarily (for a single trip) as well as permanently by the dealer (according to article 3.3).

In this regard, a survey was conducted (through a questionnaire on a sample of parents of children aged 0 to 4 years)[33].

The study found that 63% of parents would be in favor of the permanent deactivation, even for a fee, of the anti-abandonment function, with the possibility of reintroducing it if necessary; on the other hand, 37% of the interviewees were negative on this point.

Considering that these devices are in the planning phase, it is desirable that car manufacturers undertake to find innovative technological solutions that guarantee maximum safety for minors in the car, regardless of parental supervision.

5. The lack of clarity of the information from a private law point of view: linguistic error vs obstacle/defective error in view of the evolution of the category.

Technological development, in fact, does not mark the end of the law, if something, being able to determine the obsolescence of certain rules that are opposed, more often, the appearance of new legal problems, to solve which is necessary the intervention of the interpreter or the legislator.

In this case, a major problem is the lack of clarity of information, which may lead the contractor to make a mistake. In this aspect it is useful to make a small general premise followed by examples based on the cases previously considered.

According to an authoritative author[34], by mistake a false representation of the party with regard to the contract or its assumptions must be understood. It is the cause of cancellation of the contract when it is essential and recognizable (according to the article 1428 of civil code).

It is necessary to distinguish the error in the following categories:

---

[32] Assessment Protocol- Child Presence detection – Draft. Version XXX, 26th September 2019.
Article 3.3: "*long term deactivation is only allowed for direct and indirect sensing systems and must be performed by a dealer. The inactive status of the system must be indicated by a dedicated tell- tele or text warning that is permanently visible for the duration of all journeys*".

[33] The questionnaire revealed that 96% of the parents interviewed were aware of the introduction of the obligation of child presence detection device. For more information, see L Aulino, 'La sicurezza dei minori in automobile nello sviluppo della guida assistita: dalla disattivazione air-bag al dispositivo anti-abbandono' (n. 30).

[34] CM Bianca, *Diritto civile. Il contratto,* 3 (3th edn., Giuffrè, 2019) 601 ff.

- *defective error* (or error of reason), which relates to the formation of the will of the party. In fact, the contract would not have wanted to conclude without the error of the party.
- *obstacle error*: concerning the declaration of the party. It is the case which the contracting party has properly formed its will but it has been incorrectly declared or transmitted[35].

In addition, there is a further distinction between:

- a *factual error* which falls on the contractual elements or external circumstances;
- *error of law*, which falls on legal rules.

The error that falls on the contractual elements is presented as the divergence between the objective meaning of the contract and the meaning that the party gives to it.

This would be the error that would be incurred for lack of clarity of information.

In order to be a cause of annulment of the contract, the error must be essential, so it must be of decisive importance according to an objective assessment[36].

The error must also be recognizable by the other contractor (according to the article 1431 of civil code).

It should be admitted that it could be complicated to adopt the civil regulation of error with regard to autonomous vehicles. A couple of examples are worth taking from the analysis in the previous paragraphs.

First of all, it is considered the case in which it is deemed necessary to give consent to the treatment in the autonomous vehicle. The consent is necessarily an essential element of the contract, which will presumably be considered and perfected after the stage of the mere sale of the vehicle, in order to further personalize these aspects in relation to the vehicle owner's profile.

Therefore, necessarily there will be a number of options, including some optional, which the driver may or may not select by providing a split consent in a sense. After all, it is possible to imagine that the car manufacturer will ask for consent not only for that data processing necessary for the operation of the same and its sensors, but also for research and development purposes within the company or sell them to third parties.

For each of these hypotheses it will be necessary to give consent separately.

If the manner in which you provide consent should be digital and "cryptic", it is highly likely that the driver may inadvertently provide consent to all types of processing rather than only to those desired.

In such a case it would not be illogical to think that there is an error:

1) *obstacle* error, although it has formed its own will, because of the cryptic nature of the system adopted, it has been transmitted incorrectly;
2) *factual* error, involving a contractual element;
3) *essential* error, since consent to the processing of data is an essential element of the contract in order to allow the proper functioning of a level CAV from the third party up.

This conclusion is reached on the basis that data protection is often perceived by the data subject as being unrelated to the economic operation he is undertaking. If this is true, the information can take on the role not only of filling the information asymmetry but also of starting the control of data subject on the procedure on which the processing activity takes place.

A consent expressed unconsciously due to an unsuitable method of collection of the same

[35] MC Diener, *Il contratto in generale* (2th edn., Giuffrè, 2011) 805,806.

[36] The non-essential error does not invalidate the contract but can be relevant in terms of pre-contractual liability. On the point, E Quadri, *La rettifica del contratto* (Milano 1973) 77.

could be precisely understood as an obstacle error because the will, having already formed, is then transmitted/declared in an unclear way.

Consequently, with a view to dissuasion, the interpretative extension of the obstacle error category is suggested.

There is also another particular situation, concerning errors that occur after the conclusion of the contract. It is useful to take the example of the ADAS.

If the ADAS does not clearly provide the information necessary for its proper use while it is active, there will be an error.

This is an error in the transmission of information occurred after the conclusion of the contract, so will be of a linguistic nature and will be unrelated to the completion of the contractual relationship.

It can be, in fact, a critical information provided by means of a light too similar to another, a sound signal easily confused with another, a tactile signal (vibration) weak enough not to be perceived in the presence of roads that cause a high level of vibrations and shocks to the overall structure of the autonomous vehicle.

These situations of error in the providing of information could also cause road accidents, the liability of which should be ascertained.

Obviously, it will be necessary to verify on a case-by-case basis, balancing the duties of the manufacturer with the diligence of the vehicle user, but, however, it concerns an error which, unlike the previous ones, is purely linguistic and communicative error.

Nevertheless, this is of considerable importance. It is an error, albeit a linguistic one, but it concerns a particularly important system of the vehicle.

The CAV's ADAS case, so, implies an obsolescence of the normal legal categories (since it will not be enough to reason in a traditional way).

In fact, if the error occurring after the conclusion of the contract, we have to admit that we cannot lead back that error to its classical categories described before. We can no more reason in terms of defective or obstacle error because these are very specific types of errors.

So it is necessary to find another category of error which considers those errors occurring after the completion of the contractual relationship.

This means that is necessary a rethinking of the error category, perhaps introducing new concepts, with reference to the "language" and the transmission of information trying to overcome the link with the phase of completion of the contract.

6. Hypothesis of solution in the design: the legal design methodology.

In this context it is considerable of the role of design.

The most important features of a good design are: visibility (so how to identify and perform possible actions) and comprehensibility of commands[37].

The interfaces between technology and people should not only meet legal and ergonomic technical needs but should also consider the experience and quality of interaction. They should be understandable and easy to use.

The development of new technologies has led people to be frustrated by the complexity of everyday things, precisely because they generate confusion, continuous errors, and an endless cycle of updating systems.

Some authors propose the adoption of human-centered design (HCM) as a solution. It is an approach that starts from human needs, skills and behaviors, which then adapts the

[37] D Norman, *La caffettiera del masochista. Il design degli oggetti quotidiani* (Giunti, 2019).

design[38].

Good design therefore requires good communication, especially from machine to person (indicating what actions are possible, what happened and what is about to happen).

Briefly, there is a good design when the machine alerts a problem to the human that understands it, intervenes and solves the problem.

This is also because the fact that the legal information is not clear and immediate in it is understanding contrasts with the need to ensure a high degree of Situation awareness[39] in the operational framework in which the user moves.

Inadequate SA is one of the main causes of accidents attributed to human error, so users should be guaranteed a complete SA, accurate and up-to-date at all times[40].

In this context, the theme of legal design[41], a human-centred methodology that aims to achieve an effective visualization of a legal content, facilitating communication and understanding through the use of textual, paratextual elements, and information visualization[42].

The legal design approach follows the principles of clarity, transparency, awareness, immediacy of information and understanding of the text. These principles belong both to the Italian legal culture[43] and more generally to the European one[44].

---

[38] Ibid, 25-28. Anthropocentric design means starting from a good knowledge of human beings and the needs that the project intends to satisfy. This knowledge comes mainly from observation, because people are often unaware of their true needs and difficulties..

[39] The *situational awareness* (SA) is a metric related to the world of cognitive ergonomics that refers to the understanding of environmental elements in a given dimension space - time for decision makers. This concept was defined by Endsley as "*the perception of environmental elements in a given space-time dimension, the understanding of their meaning, and the projection of their status in the near future*". See M. Endsley, 'Toward a Theory of Situation Awareness in Dynamic Systems' (1995) Human Factors Journal of the Human Factors and Ergonomics Society, 32,64.

[40] Understanding the meaning of information, according to the SA model, represents the answer to the question "and then?" (so what?) the data that are perceived. In particular, the Endsley model describes the states of the AS and illustrates three phases of its training: perception (level 1 SA), understanding (level 2 SA) and projection (level 3 SA).

[41] The notion of legal design was coined by Margaret Hagan in M. Hagan, 'Law By Design' (Retrieved March 2018), in *www.lawbydesign.co/en/home/*. Legal design is the application of human-centred design to the world of law, in order to promote the usability and comprehensibility of legal instruments, and in particular contracts. Legal design is a method of creating legal services, focusing on their usability, utility and involvement. It is an approach with three main resource groups - process, mentality and mechanics - to be used for legal professionals. These three resources can help design, build and test better methods of legal action, which will involve and empower both legal professionals and individual users. See M. Hagan, 'Law by Design' (Retrieved March 2018), in www.lawbydesign.co/en/home/.

[42] Information visualization is the study of visual (interactive) representations of abstract data to strengthen human cognition. Abstract data include both numerical and non-numerical data, such as text and geographic information. On the topic see: S K Card, D Mackinlay, B Shneiderman, *Readings in Information Visualization: Using Vision to Think* (Morgan Kaufmann Publishers 1999); A Kerren, JT Stasko, JD Fekete, C North, *Information Visualization – Human-Centered Issues and Perspectives* (Berlin, Springer 2008); R Mazza, *Introduction to Information Visualization* (Springer 2009); R Spence, *Information Visualization: Design for Interaction*, (Prentice Hall 2007).

[43] The Consumer Code, in some rules, stipulates compliance with the principles of transparency and clarity in the drafting of contractual clauses. Art. 35 of legislative decree n. 206/2005 (cd. consumer code), in the first paragraph, states the obligation to draw up in a clear and comprehensible manner the clauses proposed to the consumer in writing; in addition, art. 48, establishes the obligation for the trader to provide the consumer with the information in a clear and legible; art. 51, 1 co., provides that for distance contracts the trader provides the consumer with the information in simple and understandable language. In addition, the need to ensure greater awareness of legal information is also enshrined in Articles 21 and 22 of the Consumer Code.

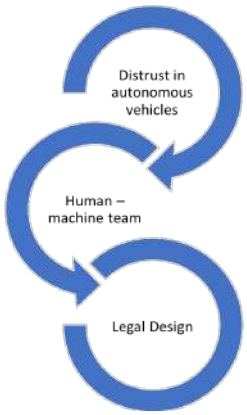
[44] The article 12 of European Regulation no. 2016/679 - on privacy and protection of personal data - provides that the data controller takes the appropriate measures to provide the data subject with all the information referred to in Articles 13 and 14 and communications referred to in art. 15-22 and 34, in a concise, transparent, intelligible and easily accessible form, in particular in the case of information specifically intended for minors.

Legal design can be seen like the final point of a very complex path, in which the jurist has understood the need to express clearly and directly following the logical architecture of the language that, it is the basis of computational thinking which, in turn, is the basis of coding (software language)[45].

It is considered that the meaning of the concept of legal design is very broad, as it includes a design technique oriented to values protected by law, cd. law by design[46].

It follows that the legal design methodology represents a possible remedy to the communication deficit of legal information provided through the vehicle.

In this regard, it would be appropriate to design human machine interfaces in this way: explain the legal information clearly and unequivocally also through an acoustic, visual or tactile signaling; avoid references to other documents; provide that such delivery methods are always supported by a previous impact assessment study of the communication construct, especially in cases where safety impacts occur, including the use of experimental models and the involvement of users as communicative effectiveness evaluators. These renewed interfaces could provide.



Conclusions.

Under a *de iure condito* perspective it is essential to adopt the design methodology law by design to a situation in which the partial or total autonomous vehicle has to provide users with compulsory legal information in order to guarantee their self-awareness.

This would also satisfy the precautionary principle and the principle of security by design and ensure mutual support and learning between the machine and the user.

Under a *de iure condendo* perspective, the European legislator should strengthen consumer protection. A rule should be introduced which punishes producer where legal information is provided to the consumer in a way that does not allow him to have a full situational awareness in the use of the product.

The GDPR also introduced the principles of privacy by design and by default where, in art. 25, requires that the design of the software minimizes the use of personal data and the risk to the data subject, both in the sense of making choices that tend to anonymize the data to be collected, both in promoting awareness of people who lend the consent to data processing. Also the W.P. 29, regarding transparency, has established the obligation to adapt the legal communication to the recipient.

[45] C Morelli, 'Avvocato 4.0: un mare di buone letture' (2020) available on *https://www.altalex.com/documents/news/2020/08/03/avvocato-4-0-un-mare-di-buone-letture.*

[46] This design methodology consists of several steps: framing the existing situation; focusing on the type of user; framing the challenge; developing ideas; understanding and prioritizing; developing a prototype; testing. See M. Hagan, 'Law by Design' (Retrieved March 2018), in *www.lawbydesign.co/en/home/*.

The same thing should be said about the cases in which the producer "causes" the error of the contractor in the phases of completion of the contract as exemplified in the example relating to the consent previously outlined.

EJPLT

La soggettività giuridica degli esseri non umani: gli animali

The legal subjectivity of non-human beings: animals

ANNA ANITA MOLLO
Ph.D at University Suor Orsola Benincasa of Naples
Lawyer

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Abstract

L'evolversi di una particolare sensibilità verso tutto ciò che è altro rispetto all'essere umano, unito allo sviluppo delle nuove tecnologie, induce a riflettere sull'adeguatezza di un sistema normative che sempre meno riflette i valori e le scelte di fondo che ispirano l'agire sociale. Allargare il campo delle riflessioni a diverse fattispecie di difficile qualificazione giuridica, che non trovano nel sistema una compiuta definizione, ha consentito di meglio analizzare il mutato rapporto tra persona umana ed animale nella vita di relazione, che tanti e diversi ambiti di studio e di disciplina è in grado di coinvolgere e che, per tale motivo, non può essere lasciato alla mera interpretazione giurisprudenziale.

…

The particular attention to what is different from human being, combined with the development of new technologies, it makes us think about the adequacy of the regulatory system, which does not reflect the values that inspire social action.

Broaden the reflections to different cases of difficult legal qualification, made it possible to better analyse the changed relationship between human being and animal in relationship life, that many and different fields of study and discipline is able to involve, and that, for this reason, it cannot be left to jurisprudential interpretation.

Keywords: Soggetti di diritto - animali - esseri non umani.

…

Legal subjects - animals - non-human beings

Summary: Premessa. – 1. La specie animale: tra qualificazione giuridica e riflessione filosofica. – 2. Il quadro normativo. – 3. Gli orientamenti giurisprudenziali – 4. Soggetto e oggetto di diritto: tra vecchie e nuove categorie giuridiche. – Conclusioni.

Premessa.

Il diritto è da sempre fondato su una concezione antropocentrica, dove la persona umana è il centro assoluto della tutela accordata; l'intera organizzazione giuridica è destinata alla persona umana, in funzione della quale l'ordinamento stesso è costituito.

Accogliendo l'insegnamento della più illustre dottrina[1], la nozione di persona non coincide

[1] BIANCA, *Diritto civile*, 2002, 135 ss.

con quella di soggetto: nel primo caso si fa riferimento a chi rileva per la sua particolare natura fisica o giuridica ed è dotata di capacità giuridica; elemento caratterizzante, nel secondo caso, è il dato formale della titolarità delle posizioni giuridiche, che possono riferirsi anche agli enti giuridici, ovvero quei soggetti che sebbene muniti di capacita giuridica generale non sono uomini.

In entrambi i casi, tuttavia, la tutela giuridica di fondo è sempre rivolta ad un interesse umano.

Ci si può allora domandare: è possibile includere gli esseri non umani tra i soggetti di diritto? Un quesito che posto in questi termini richiederebbe una trattazione ben più ampia ed approfondita delle brevi riflessioni che di qui a breve si andranno ad articolare. Alla luce di tale constatazione si è scelto di limitare l'indagine alla possibilità di riconoscere agli animali una seppur minima forma di soggettività giuridica.

Il presente contributo nasce, pertanto, dalla volontà di indagare, al di là della lettera del codice civile, se vi siano allo stato elementi che consentano di superare la tradizionale visione dell'animale quale "*res*", in modo che la relativa tutela non si ponga più in una posizione deteriore rispetto alla protezione degli interessi facenti capo all'uomo, da sempre ragione ultima dell'ordinamento giuridico.

Il mutato sentire sociale ed il diverso modo di rapportarsi al modo animale, infatti, non può lasciare indifferente il giurista che deve prendere atto dell'importanza che tali esseri viventi, seppure non umani, hanno assunto per la vita di molte persone, non solo da un punto di vista affettivo (si pensi agli animali da pet-therapy, da riabilitazione o per disabili).

1. La specie animale: tra qualificazione giuridica e riflessione filosofica.

La corretta qualificazione dello *status* degli animali è un tema già da diverso tempo oggetto di studio[2] ed ampiamente dibattuto, che induce ad un'attenta riflessione sulle categorie giuridiche tradizionali e sulla loro adeguatezza a dare risposta alla mutata sensibilità verso il mondo animale.

Diverse ed articolate sono le ricostruzioni proposte al riguardo, in ciò potendosi leggere la difficoltà di ritrovare un accordo riguardo la considerazione da riservare alla specie animale; posizioni tanto disomogenee che confermano la complessità delle implicazioni che tale tema porta con sé, che non vanno ad incidere soltanto sui diversi settori del diritto privato ma impongono, inevitabilmente, anche considerazioni di carattere non strettamente giuridico.

E' bene mettere in evidenza, pertanto, che nell'ambito della riflessione degli studiosi del diritto, accanto alle posizioni più prudenti con cui si sottolinea che gli animali non siano certamente riconducibili alla categoria delle cose inanimate[3] ma che sia necessario tutelare il loro benessere pur senza spingersi fino al punto di considerarli titolari di posizioni giuridiche[4], si pongono visioni maggiormente evolutive che considerano gli animali titolari di una vera e propria soggettività giuridica che consente di imputare direttamente alla loro sfera giuridica diritti ed interessi[5]. Più in particolare, vi è chi ritiene possibile equiparare la sfera

---

[2] GORETTI, *L'animale quale soggetto di diritto*, in *Riv. Fil*, 1928, 348.

[3] GAMBARO, *I beni*, in *Tratt. Dir. Civ. Comm*, Cicu, Messineo, Mengoni, continuato da P. Schlesinger, 2012, 216 ss.

[4] SIRISI, *Il benessere degli animali nel Trattato di Lisbona*, in *Riv. dir. agrario*, 2011, 220 ss.; MAZZONI, *I diritti degli animali gli animali sono cose o soggetti di diritto?*, in *Mannucci - Tallacchini, Per un Codice degli animali*, 2001, 111 ss.; ZATTI, *Chi è il "padrone" del cane ?*, in *Nuova giur. civ. comm.*, 1995, 137 ss; BALOCCHI, voce *Animali (protezione degli)*, in *Enc. Giur. Treccani*, 1988; FALZEA, *I fatti giuridici della vita materiale*, in *Riv. dir. civ.*, 1982, 496 ss.

[5] PARINI, *La tutela degli animali di affezione all'interno del nostro ordinamento: "le metamorfosi"*, in *Rass. dir. civ.*, 2017, 1548 ss; MARTINI, *La configurabilità della soggettività animale: un possibile esito del processo di giuridificazione dell'interesse alla loro proiezione*, in *Riv. crit. dir. priv.*, 2017, 109 ss; RESCIGNO, *I diritti degli animali. Da res a soggetti*, 2014, 89 ss;

giuridica degli animali alla particolare situazione degli incapaci, individuando nei limiti ad agire ed a soddisfare i propri interessi[6] un elemento comune alle due fattispecie.

Non sostengono, al contrario, la linea di pensiero appena illustrata coloro che, in applicazione delle norme codicistiche, ritengono che gli animali non possano rientrare nella categoria dei soggetti del diritto in quanto non godono di capacità giuridica[7]. A tale interpretazione è stato obiettato che la soggettività giuridica sia il risultato di scelte operate dal legislatore in un dato momento storico, ma che non vi siano nel sistema elementi tali da indurre l'interprete a discorrere di soggetti di diritto riferendosi unicamente agli esseri umani[8].

Per tale motivo, se si vuole discorrere della corretta qualificazione giuridica degli animali, non bisogna soffermarsi sulle qualità degli stessi quanto, piuttosto, sulla valutazione e sui valori che il legislatore decide di porre a base della sua azione[9].

Come accennato in precedenza, le teorizzazioni giuridiche sulla soggettività degli animali non possono prescindere dalla considerazione delle questioni etiche, morali e filosofiche sottese al tema trattato.

E' in tale ambito, infatti, prima ancora che per il diritto, che si è posto il problema di una diverso modo di intendere il rapporto tra l'uomo e gli altri esseri viventi che da questi si distinguono.

In risposta alla più risalente tradizione filosofica[10] che, in ragione delle diverse e non comparabili capacità cognitive, ha da sempre ricostruito il rapporto tra esseri umani e animali in ragione della prevalenza assoluta dell'uomo e dei suoi interessi, si è pian piano sviluppano un primo cambiamento di prospettiva in considerazione della capacità degli animali di provare sofferenza[11].

Si è così elaborata la logica utilitarista[12], che sostiene la pari ordinazione sul piano etico degli interessi degli animali e degli umani, richiamando l'attenzione sulla necessità che questi ultimi non arrechino agli altri esseri viventi, non solo agli animali, inutili travagli in considerazione del fatto che si tratti di esseri in grado di percepire quanto accade loro.

Ritenere gli animali titolari di un vero e proprio diritto alla vita ed al benessere ha poi contribuito a fondare il Movimento per i diritti animali, che non considera accettabile l'impiego di animali per sperimentazioni scientifiche che possono provocare loro morte o

---

Id, *Una nuova frontiera per i diritti esistenziali: gli esseri animali*, in *Giur. cost.,* 2006, 3189; GASPARIN, *La dicotomia "persona - cosa" e gli animali*, in *La questione animale*, II, in *Tratt. Biodiritto Rodotà - Zatti*, 2011, 295 ss.;; per un utile spunto comparatistico cfr. anche GARATTI, *La questione animale e le funzioni della responsabilità civile*, in *Contr. e impr. Europa*, 2014, II, 735 ss.

[6] VADALÀ, *Prospettazione storico-evolutiva dei diritti degli animali*, in *Giust. civ*., 2017, 549 ss.; VALASTRO, *La tutela giuridica degli animali e i suoi livelli*, in *Quad. cost*., 2006, 69.

[7] BIANCA, *cit*., 214. Considera gli animali quali mere *res* anche BALOCCHI, *Animali (protezione degli),* in *Enc. Giur. Treccani*, 1988, 1 ss.

[8] GALLO, voce *Soggetto di diritto*, in *Dig. Civ*., 2011, 840.

[9] MARTINI, *cit.,* 109 ss.

[10] Per una compiuta ricostruzione del pensiero filosofico nella società antica e della protezione giuridica che ivi gli animali ricevevano in funzione delle utilità che gli uomini da loro potevano trarre MARTINI, *cit*., 126 ss, il quale fa riferimento al pensiero di Aristotele, Cartesio, Locke, Leibniz e Kant che, con diverse argomentazioni, negano la soggettività degli animali.

[11] Le prime riflessioni in merito sono riconducibili al filosofo e giurista londinese BENTHAM, *Introduzione ai principi della morale e della legislazione*, opera pubblicata per la prima volta nel 1789.

[12] Il principale esponente della corrente di pensiero utilitarista è il filosofo Peter Singer che intorno alla metà degli anni settanta pubblicava per la prima volta la sua opera *Animal Liberation. Towards ad End to Man's Inhumanity to Animals*, tradotta in italiano in SINGER*, Liberazione animale: il manifesto di un movimento diffuso in tutto il mondo*, 2015, che riprende il pensiero di Bentham.

sofferenza[13]. Diversi sono, infine, coloro che ritengono che gli uomini e gli animali appartengano ad un'unica comunità in cui però è l'uomo che deve tendere ad una gestione responsabile delle diverse esigenze[14].

Le più recenti impostazioni filosofiche del tema in questione, infine, propendono per una qualificazione differenziata della sfera individuale degli animali e degli esseri umani, ciò in quanto non occorre essere simile all'uomo per meritare considerazione[15] né porsi dal loro punto di vista[16].

Da quanto detto, dunque, pare potersi cogliere, anche da un punto di vista etico-filosofico una varietà di posizioni che, per quanto non riconducibili ad unità, rappresentano in ogni caso il sostrato logico e culturale di una riflessione giuridica sul punto e di un auspicabile intervento legislativo al riguardo.

2. Il quadro normativo.

Oltre alla riflessione giuridica anche le scelte operative del legislatore, non solo a livello nazionale, sono state fortemente influenzate dall'evolversi della società e dei valori che ne costituiscono il fondamento. Il mutato rapporto tra uomo e animale nella vita di relazione ha indotto delle rilevanti, per quanto parziali e spesso contraddittorie, modifiche del quadro normativo.

Volgendo lo sguardo, *in primis*, al nostro ordinamento giuridico, dalla lettura delle norme tutt'ora vigenti del codice civile se ne ricava una qualificazione della sfera giuridica degli animali certamente non più corrispondente al diverso modo di concepire gli esseri viventi non umani cui si è fatto cenno. Ci si riferisce in particolare agli articoli da 923 a 926 c.c.: tali disposizioni, infatti, qualificando gli animali come possibile oggetto di un acquisto a titolo originario per occupazione o invenzione, confermano la volontà del legislatore di far rientrare gli animali nella categoria dei beni piuttosto che in quella dei soggetti[17]; d'altro canto, dalla lettura dell'art. 812 c.c. si ricava per esclusione che gli animali sono qualificabili come beni mobili e quindi come cose che possono formare oggetto di diritti.

Tale impostazione, chiaro riflesso del momento storico in cui il codice è stato emanato e che considera gli animali come oggetti di diritto rispetto ai quali il proprietario può agire a loro tutela in quanto cose di cui risulta titolare, ha manifestato la sua inadeguatezza a cominciare dagli anni novanta del secolo scorso quando, sul diverso versante della legislazione speciale, l'intervento si è focalizzato sulla tutela degli animali da affezione[18] e lotta al randagismo.

---

[13] La c.d. "teoria dei diritti" si deve a REGAN e alla sua opera *The Case for animal Rights*, pubblicata per la prima volta nel 1983.

[14] Si tratta della corrente di pensiero c.d. dell'"etica della responsabilità umana" che vede tra i suoi esponenti PASSMORE, *Man's Responsability for Nature*, 1980; MIDGLEY, *Animals and why they matter*, 1984.

[15] BATTAGLIA, *Approccio delle capacità e bioetica animale*, in Castiglione, Lombardi, Vallauri (a cura di), *La questione animale*, 2012, 79 ss.

[16] D'AGOSTINO, *I diritti degli animali*, in *Riv. int. Fil. Dir.*, 1994, 78 ss.

[17] GIRINO, voce *Occupazione (diritto civile)* in *Nuoviss. Dig. it*, 1965, 733 ss fa notare come sebbene il legislatore si occupi degli animali unitamente agli altri beni che possono formare oggetto di diritti, tuttavia abbia per questi individuato ipotesi di acquisto atipiche che prevedono un iter procedimentale proprio e diverso dalle altre fattispecie.

[18] Gli interventi normativi in materia di animali spesso distinguono tra animali da affezione (ovvero gli animali tenuti per compagnia ma non per fini produttivi di cui all'articolo 1, comma 2 del D.p.r. 28 febbraio 2003) ed animali da reddito, ovvero allevati e custoditi per la produzione, ad esempio di alimenti, di prodotti destinati al commercio o per scopi agricoli (di cui all'articolo 1, comma 2, lettera a) del D.lgs. 26 marzo 2001, n. 146). Nella prospettiva qui percorsa di valutare quale sia l'esatta qualificazione giuridica degli animali tale distinzione non assume alcuna rilevanza, volendo estendere le considerazioni in merito agli animali intesi come specie, senza alcuna distinzione.

Con l'emanazione della legge 14 agosto 1991, n. 281[19] si è così stabilito che lo Stato, al fine di favorire la corretta convivenza tra uomo e animale, di tutelare la salute pubblica e l'ambiente, deve promuovere e disciplinare la tutela degli animali d'affezione, condannando gli atti di crudeltà contro gli stessi, i maltrattamenti e il loro abbandono. Tale intervento normativo è degno di nota in quanto ha stabilito un principio molto importante e di portata generale, ovvero il divieto di procurare inutilmente sofferenza ad altri esseri viventi sensibili, principi questi definiti "fondamentali" da una recente circolare ministeriale (C.M. 23 maggio 20199).Tale iniziale apertura, tuttavia, per decenni è rimasta un'eccezione, non seguita da altri interventi rilevanti. Solo nel 2010, con il nuovo Codice delle Strada si è imposto un obbligo di soccorso a favore degli animali feriti vittime di incidenti, cui si aggiungono una serie di norme a protezione degli animali anche non da affezione[20].

Successivamente, invece, le scelte del legislatore appaiono alquanto contradditorie se si analizzano una serie di norme che sembrano essere ispirate da un'esigenza di tutela dell'uomo più che dell'animale. In questo senso, nel 2011, con il Codice del Consumo (d.lgs. 79/2011), si è favorito l'ingresso agli animali domestici nei luoghi aperti al pubblico dei turisti; del pari, la legge 11 dicembre 2012, n. 220, di riforma della disciplina condominiale ed in particolare dell'art. 1138, ha stabilito che il regolamento condominiale non possa vietare di possedere o detenere animali domestici[21]. Con la legge 28 dicembre 2015, n. 221, inoltre, si è stabilito che gli animali da compagnia e per fini terapeutici non sono pignorabili in quanto beni che hanno un valore morale ed affettivo. In altre parole, il legislatore non impedisce il pignoramento degli animali in quanto li considera soggetti di diritto ma, al contrario, confermando l'inquadramento giuridico degli stessi in ambito civilistico quali mere cose, nel tentativo di tutelare ancora una volta l'uomo e non l'animale, mette in evidenza il legame affettivo che tra questi inevitabilmente si crea, senza tuttavia operare alcuna scelta di principio in merito alla distinzione tra gli animali e le *res* inanimate di cui si consente il pignoramento[22].

Il legislatore penale, dal canto suo, dapprima con la legge n. 189/2004, ha introdotto nel titolo IX *bis* del codice penale varie ipotesi delittuose a tutela del sentimento per gli animali[23]. Da ultimo, con la legge n. 201/2010, di ratifica della Convenzione del Consiglio d'Europa del 1987 relativa alla protezione degli animali, c'è stato un ulteriore inasprito delle pene per i delitti di uccisione e di maltrattamento di animali, oltre all'introduzione del nuovo reato di traffico illecito di animali da compagnia.

---

[19] L'importanza del testo normativo citato è collegata anche al particolare effetto da essa prodotto ovvero di aver sottratto cani e gatti dalla vivisezione e sperimentazione animale e per aver accomunato la tutela degli animali alla salvaguardia dell'ambiente. Rilevante a tale riguardo un recente ricorso alla Corte Costituzionale per violazione ad opera della legge regionale della Basilicata n. 46/2018 dei principi stabiliti dalla legge 281/1991 nonché alcune proposte di modifica degli articoli 9 e 32 della Costituzione (Relazione del 30 gennaio 2003 sui Ddl n. 553, 1658).

[20] D.Lgs. 181/2010, di attuazione della Direttiva UE 2007/43, per la protezione dei polli allevati per la produzione di carne; D.Lgs 122/2011, di attuazione della Direttiva UE 2008/120 per la protezione dei suini in allevamento. L'art. 49 d. lgs. 47/2010 ha introdotto il divieto di commercializzazione di pellicce di cane e gatto**,** mentre l'art. 2 l. 189/2004 il divieto di commercio di prodotti derivati dalle foche**.**

[21] Rilievi critici sulla riforma sono stati mossi da CUFFARO, *L'eccezione e la regola: il comma 5 dell'art. 1138 c.c.*, in *Giur. It.* 2013, 1966 ss; TRIOLA, *Il Nuovo Condominio*, 2013, 476.

[22] PARINI, *cit.*, 1554, il quale acutamente rileva che la formulazione letterale della norma renderebbe ancora possibile il pignoramento di animali non solo da reddito ma anche quelli da affezione, ma che non sono suscettibili di essere ospitati presso la casa del debitore. Si pensi ai cani e ai gatti allevati presso apposite strutture o ai cavalli tenuti presso il maneggio.

[23] Il reato di uccisione di animali disciplinato dall'art. 554 bis ha sostituito la precedente fattispecie di cui all'art. 727 c.p., mentre il reato di maltrattamento di animali, di cui all'art. 544 ter, non costituisce più una contravvenzione ma un delitto, con conseguente inasprimento del regime sanzionatorio. Inoltre, sono stati introdotti anche il reato di *doping* a danno degli animali nonché l'organizzazione e la promozione di spettacoli e manifestazioni che comportino strazio o sevizie per gli animali

Uscendo fuori dal contesto nazionale, il primo provvedimento rilevante è stata la Dichiarazione Universale dei Diritti dell'Animale [24] con la quale, pur senza obbligare giuridicamente alcuno Stato, si invitava al rispetto di ogni forma di vita da parte dell'uomo.

Diverse sono state le convenzioni adottate nell'ambito del Consiglio d'Europa[25] ma l'intervento più importante, che ha influenzato anche il nostro legislatore verso le aperture sopra esaminate, è arrivato dall'Unione Europea; il Trattato di Lisbona, all'art. 13[26], ha infatti stabilito che gli animali sono "esseri senzienti", capaci come gli uomini di provare sofferenza e dolore, impegnando per la prima volta tutti gli Stati Membri ad assicurare agli animali una condizione di benessere comprensiva anche della dimensione morale.

Ma il Trattato di Lisbona diventa di fondamentale importanza anche nell'ottica di una breve quanto necessaria analisi della Direttiva 2010/63/UE del Parlamento Europeo e del Consiglio del 22 settembre 2010 sulla protezione degli animali utilizzati a fini scientifici. La *ratio* di tale normativa, nell'intento di dare attuazione al principio del benessere animale, era ispirata all'uniformazione nei diversi Stati Membri della normativa in materia di sperimentazione animale, garantendo al contempo il corretto funzionamento del mercato interno. Proprio il bilanciamento tra queste due opposte esigenze pare rappresenti la principale criticità di un testo normativo che, sebbene richiami più volte al suo interno il principio di cui all'articolo 13 del Trattato di Lisbona[27], appare per molti versi il risultato di scelte politiche che non sempre hanno avuto come scopo prioritario la tutela del benessere animale[28] ma che, al contrario hanno introdotto un divieto di sperimentazione sugli animali che nelle ipotesi specificamente individuate è ampiamente derogabile[29].

---

[24] Proclamata a Parigi il 15 ottobre 1978.

[25] Convenzione europea sulla protezione degli animali durante il trasporto internazionale firmata a Parigi il 13 dicembre 1968; Convenzione europea sulla protezione degli animali negli allevamenti sottoscritta a Strasburgo il 10 marzo 1976; Convenzione europea sulla protezione degli animali da macello approvata a Strasburgo il 10 maggio 1979; Convenzione europea sulla protezione degli animali vertebrati utilizzati a fini sperimentali o ad altri fini scientifici del 18 marzo 1986; Convenzione europea per la protezione degli animali da compagnia firmata a Strasburgo il 13 novembre 1987.

[26] L'art. 13 del Trattato di Lisbona rappresenta un traguardo raggiunto anche grazie ad alcuni precedenti passaggi di assoluta rilevanza. Dapprima la Dichiarazione n. 24 allegata al trattato di Maastricht invitava gli Stati Membri a tener conto del benessere animale nel contesto della politica agricola comune, dei trasporti, del mercato interno, della ricerca e dello sviluppo tecnologico. Successivamente, con il Protocollo sulla Protezione e il benessere degli animali, allegato al Trattato di Amsterdam, si fa per la prima volta riferimento, era il 1997, agli animali come esseri senzienti.

[27] Proprio in funzione di dare concreta attuazione a tale principio l'articolo 4 della direttiva 2010/63/UE recepisce il principio delle "tre R" (replacement, reduction and refinement) di BURCH, *The principle of human experimental technique*, 1959.

[28] Sull'analisi critica di tale direttiva: PUOTI, *L'attuazione della direttiva 2010/63/UE sulla protezione degli animali da sperimentazione nel contest dell'armonizzazione del mercato interno e il futuro della ricercar in Italia*, in *Studi sull'integrazione europea*, 2016, 301 ss.; FORASTIERO, *La tutela giuridica degli animali da esperimento: riflessioni sull'attuazione in Italia della direttiva 2010/63/UE*, in *Studi sull'integrazione europea*, 2014, 565 ss.; A.A.V.V., *Sperimentazione animale: aspetti teorici, normativi e applicativi della nuova direttiva europea 2010/63,* a cura di Manciocco, Romano, Zoratto, Branchi, Berry, 2011.

[29] In particolare l'articolo 5 della direttiva 2010/63/UE prevede che sia consentita: la ricerca di base, per la cui conduzione non è previsto alcun vincolo; la ricerca applicata o traslazionale volta alla profilassi, alla prevenzione, alla diagnosi o alla cura delle malattie, del cattivo stato di salute o di altre anomalie, o dei loro effetti sugli esseri umani, sugli animali o sulle piante; alla valutazione, alla rilevazione, al controllo o alle modificazioni delle condizioni fisiologiche negli esseri umani, negli animali o nelle piante; oppure al benessere degli animali ed al miglioramento delle condizioni di produzione per gli animali allevati a fini agronomici; la realizzazione di uno degli scopi di cui al punto precedente nell'ambito dello sviluppo, della produzione o delle prove di qualità, di efficacia e di innocuità dei farmaci, dei prodotti alimentari, dei mangimi e di altre sostanze o prodotti; la protezione dell'ambiente naturale, nell'interesse della salute o del benessere degli esseri umani o degli animali; la ricerca finalizzata alla conservazione delle specie; l'insegnamento superiore o la formazione ai

Tale direttiva è stata recepita nel nostro ordinamento giuridico con il d.lgs. 4 marzo 2014, n. 26[30] che si caratterizza per l'introduzione di una disciplina per alcuni versi più rigorosa di quella delineata nel testo normativo di fonte comunitaria[31] ma che, per altri aspetti, è apparsa deludente in quanto orientata perlopiù a ridurre ed impedire la sperimentazione, più che ad incentivare l'utilizzo di metodi di ricerca che prevedano procedure alternative che non consentano l'impiego di animali (*replacement*). Ciò, evidentemente, non può che determinare un impatto del tutto negativo sulla ricerca scientifica che in tal modo rimane legata a metodi e procedure ormai vecchie e superate[32].

Da ultimo, occorre dare conto di un recente disegno di legge con il quale, sul modello tedesco[33], si intenderebbe modificare gli articoli 9 e 117 della Costituzione in modo tale da dare copertura costituzionale ai diritti animali[34].

3. Gli orientamenti giurisprudenziali.

Anche dal formante giurisprudenziale sono stati forniti importanti spunti verso un'evoluzione dell'interpretazione più risalente della qualificazione giuridica degli animali come meri beni.

Soprattutto l'ambito delle relazioni familiari, nella loro fase patologica, è stato maggiormente prolifico di decisioni di rilevante interesse nella prospettiva qui analizzata.

Diversi sono stati i giudici, con decisioni anche molti recenti, che si sono espressi nel senso di non voler considerare gli animali da compagnia alla stregua degli altri beni mobili di cui occorre occuparsi in funzione divisoria nell'ambito di un giudizio di separazione o di divorzio.

Tra le decisioni più note e rilevanti vi è sicuramente quella del Tribunale di Milano del marzo del 2013, con la quale il giudice, omologando un accordo di separazione che prevedeva al suo interno anche l'affidamento ed il mantenimento economico dei gatti di famiglia, ha messo in evidenza come gli animali, sulla scorta del dato normativo di cui al Trattato di Lisbona del 13 dicembre 2007, non possano più considerarsi delle mere cose bensì "esseri senzienti". Ciò giustifica ed autorizza il giudice ad accogliere in sede di separazione accordi in cui legittimamente i coniugi intendano regolare la permanenza degli animali domestici presso la rispettiva abitazione ed il relativo mantenimento economico.

Diverse sono state le sentenze di merito che hanno messo in evidenza come, in assenza di una precisa disciplina normativa al riguardo, soltanto l'accordo tra i coniugi, sia in sede di separazione che di divorzio, può legittimare il giudice a decidere in merito alla possibilità di

---

fini dell'acquisizione, del mantenimento o del miglioramento di competenze professionali; le indagini medico-legali.

[30] Tale testo normativo ha sostituito il d.lgs. 116/1992 che recepiva la precedente direttiva 86/09/CEE.

[31] La normativa italiana di recepimento della c.d. "direttiva antivivisezione" introduce il divieto di ricerche sugli xenotrapianti e sulle sostanze d'abuso (art. 5 par.2); è tassativamente esclusa la sperimentazione su scimmie antropomorfe (art. 7 par. 3) nonché la sperimentazione quale metodo della didattica nelle scuole primarie, secondarie e nei corsi universitari e nella formazione professionale. E', altresì, vietato sottoporre a sperimentazione gli animali resi afoni (art. 14). Proprio in considerazione del maggior rigore che il d.lgs. 26/2014 garantisce nel nostro sistema giuridico rispetto a quanto stabilito dalla direttiva antivivisezione, diverse sono state le critiche di chi ritiene eccessivi i limiti alla sperimentazione introdotti dalla normativa interna, in quanto andrebbero a discapito della ricerca scientifica volta a trovare nuove cure ed a favorire un generale miglioramento delle condizioni di vita e di salute delle persone affette da malattie rare e incurabili. Così MEOLA, *Al crocevia tra i diritti delle diverse specie: a proposito degli xenotrapianti*, in *Rivista di Biodiritto*, 2019, 466 ss.

[32] KUAN, *Vivisezione. Dati allarmanti su aumento test dolorosi e stabulari in Italia. Governo indirizzi la ricerca verso metodi alternativi*, 2015, reperibile al sito www.lav.it.

[33] Il 26 luglio 2002 è stato introdotto dal Parlamento tedesco l'articolo 20a del Grundgesetz che ha inserito la tutela e la protezione degli animali tra i fini dell'azione statale.

[34] Proposta di legge costituzionale XVIII legislatura del 23 marzo 2018 di iniziativa dell'On.le Brambilla.

assegnare gli animali domestici ad uno dei due coniugi[35]. Degna di nota in tale filone è sicuramente una pronuncia del Tribunale di Como[36] che, dopo aver affermato che il giudice non è tenuto ad occuparsi dell'assegnazione degli animali da affezione, precisa come un eventuale accordo sul punto non sarebbe in contrasto con alcuna norma cogente o con principi di ordine pubblico; per altro verso, il medesimo decreto contiene anche un chiaro invito ai coniugi a disciplinare in altra sede tali aspetti, oltre che un giudizio negativo circa le condizioni dell'accordo di separazione relative alla frequentazione con l'animale in via alternata che "*ricalcando impropriamente sul piano terminologico le clausole generalmente adottate in tema di affidamento, collocazione e protocollo di visita dei figli minori, il che a questo giudice pare una caduta di stile sul piano culturale*"

Di poco successiva una pronuncia del Tribunale di Roma[37] che, in applicazione di principi di diritto già espressi da due precedenti di merito[38], ritiene che nel dare prevalenza al benessere affettivo e spirituale dell'animale, in assenza di una disciplina al riguardo, si possa fare applicazione analogica delle norme in materia di affidamento dei figli minori; ciò anche quando si tratti di decidere a chi affidare l'animale domestico nell'ambito di coppie non coniugate ma soltanto conviventi, posto che dal punto di vista della tutela dell'interesse dell'animale, non ha alcuna rilevanza che le parti siano coniugate, in quanto l'affetto che questi può provare per entrambi prescinde dal regime giuridico che le legava. Oltretutto, si fa un preciso richiamo all'articolo 455 ter contenuto nella proposta di legge con la quale si vuole introdurre nel codice civile una tutela specifica per l'affido degli animali familiari in caso di separazione dei coniugi e che equipara la fattispecie della separazione dei coniugi con quella della cessazione della convivenza *more uxorio*[39]. Appare allora singolare al riguardo che, in ambito penalistico al contrario, l'equiparazione di un minore ad un animale sia stata qualificata come reato di cui all'art. 595 c.p.[40]

Solo di recente, contrariamente dalla giurisprudenza appena esaminata, anche in sede di separazione giudiziale vi è stata una pronuncia molto interessante per il profilo in questa sede esaminato: si tratta di un decreto del Presidente di sezione successivo al tentativo di conciliazione con il quale, per la prima volta, la tutela accordata agli animali ha trovato il suo fondamento non in una semplice esigenza di cura del sentimento degli animali, ma ritenendo tale aspetto come essenziale per il benessere ed il miglior sviluppo dell'*identità* degli animali[41].

Dalla lettura di tale provvedimento appare tutta la forza innovativa ed il cambio di prospettiva ancora più marcato rispetto alla precedente giurisprudenza, pure favorevole ad

---

35 Trib. Milano, 2 marzo 2011; Trib. Milano, 17 luglio 2013; Trib. Como, 3 febbraio 2016.

36 Trib. di Como, 3 febbraio 2016.

37 Trib. Roma, 15 marzo 2016.

38 Trib. Foggia, inedita, che in una causa di separazione, ha affidato il cane ad uno dei coniugi, concedendo all'altro il diritto di visita per alcune ore determinate nel corso della giornata; Trib. Cremona, inedita, che sempre in un giudizio di separazione , ha disposto l'affido condiviso del cane con obbligo di suddivisione al 50% delle spese per il suo mantenimento.

39 Proposta di legge XVII legislatura n. 960, presentata il 16 maggio 2013 d'iniziativa dei deputati Giammanco, Brambilla, Catanoso Genoese con la quale si vorrebbe introdurre la seguente disposizione nel codice civile: art. 445 ter "*In caso di separazione dei coniugi, proprietari di un animale familiare, il Tribunale, in mancanza di un accordo tra le parti, a prescindere dal regime di separazione o di comunione dei beni e a quanto risultante dai documenti anagrafici dell'animale sentiti coniugi, i conviventi, la prole e, se del caso, esperti di comportamento animale, attribuisce l'affido esclusivo o condiviso dell'animale alla parte in grado di garantire il maggior benessere. Il Tribunale è competente a decidere in merito all'affido di cui al presente comma anche in caso di cessazione della convivenza more urorio*"

40 Cass., sez. V pen., 27 maggio 2019, in *DeJure*.

41 Trib. Sciacca, 19 febbraio 2019 " … *rilevato che in mancanza di accordi condivisi e sul presupposto che il sentimento per gli animali costituisce un valore meritevole di tutela, anche in relazione al benessere dell'animale stesso, assegna il gatto (omissis...) (omissis...) al resistente che dalla sommaria istruttoria appare assicurare il miglior sviluppo possibile dell'identità dell'animale ed il cane (omissis...), indipendentemente dall'eventuale intestazione risultante nel microchip, ad entrambe le parti, a settimane alterne, con spese veterinarie e straordinarie al 50%.* "

una rivalutazione della natura giuridica degli animali: in questo caso, infatti, il giudice non si è limitato a prendere in considerazione la sfera affettiva ed emotiva dell'animale ma ha a questi riferito una categoria giuridica da sempre collegata unicamente alle persone fisiche, ovvero l'identità. Gli animali sono, dunque, dotati di una identità propria, ovvero di un preciso diritto soggettivo, tra quelli fondamentali riconosciuti alle persone fisiche?

A fronte delle aperture rilevanti che si sono appena analizzate, non pochi sono i segnali della giurisprudenza che, all'opposto, tendono a confermare la visione fortemente antropocentrica che ancora resiste nel nostro codice civile. Diverse sono le sentenze relative ad animali oggetto di contratti di compravendita ai quali si è ritenuto di applicare la disciplina del Codice del Consumo[42] o casi in cui la giurisprudenza ha fatto ricordo alla categoria dell'*aliud pro alio*[43]. Infine, dando brevemente conto anche delle pronunce emesse con specifico riferimento all'ambito della responsabilità extracontrattuale per danni o uccisione dell'animale da affezione, dopo un'iniziale chiusura della giurisprudenza di legittimità che aveva negato il risarcimento del danno non patrimoniale subito dal proprietario dell'animale per mancanza di lesione di un diritto inviolabile[44], la Corti di merito più di recente hanno ammesso tale risarcimento sul presupposto che il particolare rapporto tra l'uomo e l'animale trovi tutela nell'articolo 2 della Costituzione in quanto funzionale alla libera e completa espressione della personalità dell'essere umano[45].

4. Soggetto ed oggetto di diritto: tra vecchie e nuove categorie giuridiche.

Il dualismo soggetto-*res*, che affonda le sue radici nel diritto romano e che costituisce il fondamento di tutti i codici civili che da tale tradizione giuridica derivano, ha costituito il sostrato anche della discussione in merito al riconoscimento o meno della capacità giuridica in capo al nascituro concepito.

Non è certo questa la sede per riprendere l'intero dibattito dottrinale e giurisprudenziale in merito; tuttavia, da una breve analisi delle discussioni sul punto sembra potersi trarre qualche spunto di riflessione anche nella diversa prospettiva dell'adeguatezza dell'attuale qualificazione giuridica degli animali come *res*.

Per molto tempo il nascituro concepito è rimasto in bilico tra le categorie del soggetto o dell'oggetto di diritto, imponendo un'attenta riflessione sulla insufficienza delle tradizionali categorie giuridiche ad accoglierlo.

Secondo la teoria preferibile[46], che ha trovato conferma anche nella giurisprudenza di

---

42 Cass., 25 settembre 2018, n. 22728, in *Danno e resp.*, 2019, 70 ss. con nota di BERTELLI;

43 App. Salerno, 4 agosto 2017, in *Corr. Giur.*, 2018, 1539 ss, con nota di CARRATO; Cass. 19 dicembre 2013, n. 28419, in *Mass.*, 2013, 948 ss.; Giudice di pace Napoli 22 ottobre 2008; Cass. 14 giugno 2000, n. 8126, in *Giur. it.,* 2001,, 237 ss.

44 Cass. SS.UU., 11 novembre 2008, nn. 26972, 26973, 26974, 26975, cui si erano uniformate Trib. Milano, 20 luglio 2010, n, 9453 e Trib. Roma 19 aprile 2010.

45 Trib. Pavia, 16 settembre 2016, n. 1266; Trib. Milano 5 aprile 2019 in *DeJure*

46 BIANCA, *cit.*, 221 ss; con argomentazioni in parte diverse, considera in ogni caso attuali gli interessi del concepito come soggetto OPPO, *L'inizio della vita umana*, in *Riv. dir. civ.*, 1982, 499 ss., per il quale il concepito sarebbe titolare di una capacità sottoposta alla condizione sospensiva dell'evento della nascita che retroagisce al momento del concepimento. Da tale ultima dottrina si sono mossi poi, nello stesso senso, altri illustri autori tra cui GIACOBBE, *Problemi civili e costituzionali sulla tutela della vita*, in *Dir. Fam.*, 1988, 1119 ss.; ZATTI, *Quale statuto per l'embrione?*, in *Riv. crit. dir. priv.*, 1990, 463 ss.; BUSNELLI, *L'inizio della vita umana*, in *Riv. dir. civ.*, 2004, 533 ss., che riconosce il diritto del concepito il diritto ad essere tutelato in virtù del principio costituzionale della tutela della vita umana fin dal suo inizio; secondo SANTORO PASSARELLI, *Dottrine Generali del Diritto Civile*, 2002, 26, l'attribuzione di diritti previsti dal codice civile deve essere interpretata nel senso della costituzione di un centro autonomo di rapporti giuridici in previsione ed attesa della persona. Al contrario, negano che il concepito sia soggetto di diritto titolare di capacità giuridica GAZZONI, *Manuale di diritto privato,* 2011, 123, secondo il quale il legislatore detta una tutela conservativa, in relazione ad un patrimonio attualmente privo di titolare; LIPARI,

legittimità[47], il concepito è titolare si interessi attuali che impongono il riconoscimento a suo favore non solo di una soggettività giuridica ma anche di una vera e propria capacità giuridica. Ciò in considerazione delle diverse norme con cui l'ordinamento giuridico riconosce al concepito una serie di diritti che non sono accantonati fino alla sua nascita ma sono da subito esercitati dai suoi rappresentati legali[48]; si pensi non solo alla tutela apprestata alla sfera patrimoniale ma anche a quella personale del concepito prima della nascita[49].

Nella nozione di concepito rientra anche quella di embrione non formatosi naturalmente ma in modo artificiale in laboratorio, di cui alla legge 14 febbraio 2004, n. 40[50], e ciò sia che tale embrione sia o meno impiantato nel corpo della donna, sia che si tratti di ovulo umano non fecondato in cui sia stato impiantato il nucleo di una cellula umana matura[51]. In relazione a tali fattispecie il legislatore non ha predisposto una specifica tutela, ma ha vincolato la produzione di embrioni umani al solo scopo dell'impianto e stabilito il divieto di sperimentazione su di essi e di selezione eugenetica (art. 13 della legge 14 febbraio 2004, n. 40)[52].

A differenza di quanto visto per il nascituro concepito, in relazione all'embrione non impiantato risulta ancora senza risposta l'interrogativo circa la sua esatta qualificazione giuridica, quale mero prodotto organico oppure quale destinatario di una specifica tutela in quanto frutto di un concepimento, seppure artificiale, e per tale motivo potenziale vita umana[53].

Ebbene, dall'analisi della normativa sopra condotta, non pare che rispetto alla specie animale l'ordinamento riconosca una serie di interessi la cui attualità legittimi il

Le categorie del diritto civile, 2013, 61 e ss., sul presupposto che non sia possibile distinguere la soggettività dalla personalità.

47 Cass. 11.5.2009 n. 10741. La Suprema Corte ha affermato che il nascituro è un soggetto giuridico, precisando che quella della soggettività giuridica è una nozione più ampia di quella di capacità e di personalità giuridica. Il nascituro concepito risulta in tal modo titolare di autonoma soggettiva giuridica in quanto titolare di una serie di interessi a carattere personale (diritto alla vita, alla salute, all'integrità psicofisica ed all'identità personale) già attuali anche prima della nascita, quest'ultima rappresentando soltanto il presupposto per la loro azionianbiltà in giudizio a fini risarcitori. In commento alla citata sentenza, BALLARANI, *La Cassazione riconosce la soggettività del concepito: indagine sui precedenti dottrinali per una lettura "integrata" dell'art. 1 c.c.,* in *Giust. civ*, 2009, 1159 e ss.; CRICENTI, *Il concepito soggetto di diritto ed i limiti dell'interpretazione*, in *Nuova giur. civ. comm*, 2009, 1258 e ss. Sul punto, inoltre, GALGANO, *Danno da procreazione e danno al feto, ovvero quando la montagna partorisce un topolino*, in *Contr. impr.*, 2009, 537 e ss.; BUSNELLI, *Il problema della soggettività del concepito a cinque anni dalla legge sulla procreazione medicalmente assistita*, in *Nuova giur. civ. comm*, 2010, 185 e ss. Di fondamentale importanza, nella diversa prospettiva della tutela costituzionale del concepito, Corte Cost. 18 febbraio 1975, n. 27 e Corte Cost. 28 gennaio 2005, n. 45.

48 Art. 320, co. 1, c.c. e art. 643 c.c.

49 Si pensi alla capacità di succedere (art. 462 c.c.) o di ricevere per donazione (art. 643 c.c.), alla revocazione delle disposizioni testamentarie per sopravvenienza di figli anche se il figlio è stato concepito al tempo del testamento (art. 687 c.c.), nonché all'interesse al riconoscimento anche prima della nascita (art. 254 c.c.)

50 Un'attenta analisi della legge in parola in SESTA, *Dalla libertà ai divieti: quale futuro per la legge sul- la procreazione medicalmente assistita?*, in *Corr. giur.*, 2004, 1405 ss.

51 Così BALLARANI, *Nasciturо (soggettività del)*, in *Enc. Bioetica*, 136 ss.

52 In merito ai complessi risvolti determinati dall'instaurarsi del rapporto di filiazione da tecniche di procreazione medicalmente assistita GATT, *The Question of the Genetic Identity of Individuals between National Law and the European Court of Human Rights*, in *Annals of Bioethics & Clinical Applications*, 2020, 1-2; ID, *Il problema dei minori senza identità genetica nei (vecchi e) nuovi modelli di famiglia: il conflitto tra ordine pubblico interno e c.d. ordine pubblico internazionale*, in *Familia*, 2017, 271 ss. Con particolare riferimento al caso dello scambio di embrioni CAGGIANO, *Veridicità della filiazione ed errore nella procreazione assistita. Un rapporto possibile tra interpretazione della legge e studi empirici*, 2018, 1-268.

53 Per una più ampia e puntuale analisi del problema della soggettività degli embrioni sovrannumerari e, più in generale, di altre entità non umane quali gli animali, la natura e i robot GATT, *Codex - Libro I :antropocentrismo giuridico tra natura e tecnologia*, in corso di pubblicazione. Sul punto anche una recentissima pronuncia del Tribunale di Modena del 8 maggio 2020 che ha negato il trasferimento *mortis causa* dei gameti crioconservati del marito defunto al coniuge superstite in applicazione delle norme codicistiche in materia di successione legittima.

riconoscimento in capo agli stessi di situazioni giuridiche al pari di quanto fatto per il concepito. In altre parole, non è possibile ricondurre agli animali quelle posizioni di chi è partecipe di relazioni sociali, seppure per il tramite del suo rappresentante, come nel caso del concepito, ovvero di quelle situazioni giuridiche di cui è titolare un soggetto di diritto (per come inteso nell'attuale quadro normativo).

Se in relazione all'embrione non impiantato, inoltre, che pure è suscettibile di divenire un essere umano al pari di quello concepito naturalmente, i dubbi circa la sua esatta qualificazione giuridica trovano fonte nel vuoto normativo che caratterizza tali particolari situazioni nate in seguito allo sviluppo della scienza e delle nuove tecnologie, non si comprende in che modo lo stesso vuoto di tutela, o meglio sarebbe dire una diversa per quanto risalente qualificazione in termini di *res*, possa condurre ad ipotizzare una soggettività giuridica in capo alla specie animale.

Tali brevi considerazioni per sottolineare come non appaiono condivisibili, a parere di chi scrive, le posizioni prima illustrate di quanti colgono nell'incapacità degli animali, di esprimere sé stessi e di comunicare con gli uomini, un elemento di similitudine con la situazione dell'incapace persona fisica; più nello specifico, ritenere di equiparare gli animali ai minori e, più in generale, agli incapaci, sul presupposto che sia sufficiente in entrambi i casi ricorrere al meccanismo della rappresentanza, non appare una ragionamento condivisibile, neppure se analizzato alla luce del procedimento analogico di cui all'articolo 12 preleggi.

In particolare, ai sensi del secondo comma della norma appena citata, se una controversia non può essere decisa con una precisa disposizione, si ha riguardo alle disposizioni che regolano casi simili o materie analoghe: al riguardo preme precisare che, fermo restando la necessità di tutelare il benessere animale da ogni abuso immotivato perpetrato da terzi ingiustamente, l'accertata ed incontestabile differenza, sul piano scientifico e biologico delle capacità cognitive degli esseri umani rispetto agli animali, non pare consenta di sostenere che entrambe le specie possano essere titolari dei medesimi diritti, oppure che sia possibile equiparare gli animali agli incapaci legali[54]. Non solo, in applicazione della seconda parte del secondo comma dell'articolo 12 preleggi, se il caso rimane ancora dubbio si decide secondo i principi generali dell'ordinamento giuridico: dall'analisi normativa sopra condotta non pare potersi individuare nel nostro ordinamento giuridico un principio generale che consenta di equiparare gli animali agli esseri umani.

Appaiono invece condivisibili le posizioni più caute e realistiche di ritiene che si possa parlare di "una oggettività attenuata"[55] o di un "tipo di soggettività"[56] diverso da quello che si riconosce agli esseri umani; allo stesso modo appare condivisibile l'opinione di chi, in una visione di maggiore revisione dell'impianto normativo già esistente, propone l'introduzione di una terza categoria giuridica, diversa sia dai soggetti che dalle mere *res*, con caratteristiche e peculiarità sue proprie ed al cui interno ricondurre la specie animale, con una completa differenziazione sul piano giuridico rispetto alla persona umana[57].

Conclusioni.

Alla luce dell'analisi svolta appaiono diverse le incertezze e le contraddizioni che ancora

---

[54] Sul punto MARTINI, *cit.*, 130, il quale bene mette in evidenza come tali considerazioni non hanno nulla a che fare con i diritti della specie animale.

[55] BERTELLI, *Applicabilità del codice del consumo alla compravendita di animali*, in *Danno e resp.,* 2019, 75, la quel fa rilevale che ciò basterebbe a proteggere lo *status* degli animali non essendo possibile, allo stato attuale, far coincidere soggetto ed oggetto di diritto.

[56] MARTINI, *cit.,* 134 il quale precisa come non sia possibile riconoscere agli animali la stessa soggettività degli esseri umani ma, in ogni caso, di un "tipo di soggettività".

[57] SETTANI – RUGGI, *Diritto animale, diritto degli animali e diritti degli animali. L'auspicio di un intervento riorganizzativo del legislatore tra esigenze sociali e necessità giuridiche di sistema*, in *Rivista di BioDiritto*, 2019, 488 ss.

caratterizzano il nostro sistema giuridico, che sembrano impedire una soluzione univoca[58] in merito alla possibilità di riconoscere una soggettività giuridica anche agli esseri viventi diversi dall'uomo.

Tuttavia, le contraddizioni non sono, a parere di chi scrive, riferibili alla questione animale in quanto tale, ma ad una più ampia considerazione in termini di qualificazione giuridica di tutto ciò che si differenzia dall'essere umano. In altre parole, se i valori, e le scelte che questi inducono nel legislatore, variano inevitabilmente al mutare della società e della sua evoluzione, anche tecnologica, appare plausibile ripensare alla tradizionale qualificazione degli animali in termini di meri beni e tendere ad una modifica del relativo impianto normativo.

Ciò che, al contrario, lascia perplessi è la volontà di parificare a tutti i costi gli animali agli esseri umani pur in assenza di un valido riferimento normativo, come si è cercato di dimostrare con l'analisi sopra condotta. A ciò si aggiunga che tale sforzo interpretativo non viene compiuto per quelle entità che pure sono suscettibili di diventare esseri umani viventi e per i quali appare meno difficile ritrovare elementi tali da giustificare l'applicazione in via analogica delle norme a tutela della vita umana.

In conclusione, alla luce dell'attuale quadro normativo, non pare siano riscontrabili elementi tali che consentano di poter attribuire una seppur limitata soggettività giuridica in capo agli animali, per come tale ultima categoria giuridica è attualmente configurata. Tale considerazione non impedisce, da un lato, di auspicare un intervento legislativo al riguardo, come in tutte le ipotesi in cui manca nel sistema giuridico un certo livello di protezione e disciplina per situazioni che si considerano meritevoli di tutela; dall'altro, sia consentito esprimere qualche perplessità circa la reale efficacia di un sistema di tutela a favore degli animali che non si limiti a differenziali dalle *res* inanimate ma si spinga fino al punto di qualificarli come veri e propri soggetti di diritto. Tale incertezza nasce da una riflessione sui possibili risvolti pratici di un intervento in tal senso; in altre parole, ci si chiede a chi possa arrecare beneficio un sistema di norme che consenta di configurare l'animale non come oggetto di un contratto di compravendita ma come parte dello stesso, piuttosto che come beneficiario di un lascito testamentario. Allo stato, è possibile affermare con un sufficiente grado di certezza che un sistema giuridico che consentisse di operare in tal senso non abbia come destinatario principale degli interessi in tal modo soddisfatti nuovamente l'uomo e non l'animale?

[58] ALPA E ANSALDO, *Le persone fisiche, Artt. 1-10 c.c.*, in *Cod. civ. Comm.* Schlesinger, 2013, 222 ss.

EJPLT

L'io, l'altro e il bilanciamento degli interessi nella *artificial intelligence*

The ego, the other and the balance of interests in artificial intelligence

MASSIMILIANO CICORIA
Ph.D. in Diritto Comune Patrimoniale at University Federico II of Naples
Lawyer

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Abstract

'Io' e 'altro' sono, nel diritto privato, concetti di primaria grandezza che, in un doveroso bilanciamento dei contrapposti interessi, assumono rilevanza ai fini della tutela delle singole situazioni giuridiche. L'indagine di tali assiomi è svolta partendo dai più noti diritti all'identità, immagine, riservatezza e oblio per giungere alla più recente Intelligenza Artificiale e a talune problematiche che essa solleva.

…

'Ego' and 'other' are, in private law, concepts of primary magnitude which, in a proper balancing of opposing interests, take on relevance for the purposes of protecting individual legal situations. The investigation of these axioms is carried out starting from the most well-known rights to identity, image, confidentiality and oblivion to reach the most recent Artificial Intelligence and certain problems it raises.

Keywords: Individuo - Bilanciamento di interessi - Identità - Riservatezza - Diritto all'oblio - Intelligenza artificiale.

…

Individual - Balance of interests - Identity - Privacy - Right to be forgotten - Artificial Intelligence.

Summary: Introduction – 1. Il prisma dell'identità nella vita di relazione. – 2. L'immagine di sé. – 3. Riservatezza ed accountability. – 4. La AI di terza generazione e il White Paper del Parlamento Europeo. – 5. Il bilanciamento degli interessi nella AI. – Conclusions.

Introduction.

"*L'enfer sont les autres*!" scriveva Sartre nell'opera teatrale 'A porte chiuse'. L'assunto, ancorché provocatorio, potrebbe comportare un assioma: sussiste un minimo comune denominatore tra identità, immagine, trattamento dei dati, oblio e, infine, Intelligenza Artificiale (AI), cioè l'*altro*, il diverso, il distante da me, ciò che non sono io, che è 'fuori' da me, colui al quale mi contrappongo e a cui contrappongo il mio io, i miei interessi e diritti, colui che porta suoi propri interessi confliggenti coi miei, colui che rivendica spazi, fissa o solca confini, l'entità estranea e visibile (o non) rispetto alla quale mi specchio e che consente la mia esistenza, la mia diversità rispetto a lui, la mia identità intesa come eguaglianza solo a me medesimo e, dunque, la mia stessa alterità ma non rispetto a me, bensì all'altro.

Concetto, quello di *altro*, complesso, filosoficamente impervio e giuridicamente ingombrante che reca con sé anche quelli di 'conflitto' e di 'bilanciamento di interessi'. Ne

'La metafisica dei costumi', Immanuel Kant ebbe a precisare che "l'uomo è un essere destinato alla socialità e coltivando il proprio stato sociale egli sente potente e vivo il bisogno di espansione agli altri; ma d'altro lato egli è trattenuto e avvertito dal timore dell'abuso che altri può fare di questa rivelazione dei suoi pensieri, e si vede così costretto a rinchiudere in se stesso buona parte dei suoi giudizi"[1]. Un'alternanza dunque di necessità o interessi che, a volte contrapposti, espandono o riducono le distanze tra "l'io ed il tu"[2] e che impongono sia la contemplazione "dell'essere in sé" dell'altro[3], sia il riconoscimento della soggettività dell'altro inteso, quindi, non più come mero oggetto di conoscenza, bensì come interlocutore attivo[4]. In una visione, per così dire eliocentrica, l'attenzione dello spettatore (l'io) obbliga lo sguardo a spostarsi altrove, dal me medesimo all'altro, per conciliare il mio con lo spazio altrui, nella consapevolezza che la mia esistenza è in quanto è quella dell'altro o, per dirla usando le parole di un accorto Maestro, che "Robinson Crusoe non sarebbe mai esistito senza Venerdì"[5]. E' la tematica delle cd. relazioni ociali, cioè di "ciò che sta fra i soggetti agenti e che – come tale – costituisce il loro orientarsi e agire reciproco" al fine di definire "sia la distanza sia l'integrazione degli individui che stanno in società"[6].

Il tema è amplio, assai esteso, al punto da rischiare di intravedere solo qualche albero, piuttosto che l'intera foresta. Basti dire che, nel codice civile, il concetto di *altro* è potentemente richiamato dall'art. 2043 il quale, nel postulare che "qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno", è evidentemente redatto in terza persona con un rovesciamento di prospettiva dall'io, appunto all'altro: non dunque "chi cagiona a me un danno deve risarcirmi", bensì "se io cagiono danno ad un altro devo risarcirlo". E ciò produce al contempo una sussunzione del particolare nel generale, poiché, nel principio del *neminem laedere*, si riassumono entrambi i concetti di io e di altro, laddove entrambi non dobbiamo né ricevere, né tanmeno arrecare danno ingiusto. E su questa prospettiva, cioè il rapporto confliggente tra l'io e l'altro, muovono i passi le teorie della 'responsabilità' o, meglio, della tutela civile dei diritti ed, in particolare, la diade tra *property rules* e *liability rules*. La scelta del legislatore tra tutela proprietaria e tutela di responsabilità è predeterminata non avendo riguardo alla direzione (*erga omnes* o *inter partes*) della tutela stessa, ma al bene o all'utilità tutelati: la prima avrà ragione nel caso in cui il godimento appunto del bene o dell'utilità sia 'incondizionato' in capo al titolare (io), senza il cui consenso l'altro non può, quindi, godere della *res*; la seconda, invece, non assicura un godimento eguale all'io, ma l'altro che vuole utilizzare la *res* deve sopportarne il costo o, meglio, il peso del danno cagionato dall'utilizzo[7]. Si tratta, invero, di un vero e proprio 'bilanciamento di interessi' che, a sua volta, apre il tema della omogeneità o meno degli interessi tutelati. Nel caso, difatti, in cui vi sia contrasto tra interessi della stessa natura (ad esempio, costituzionali poiché o contemplati esplicitamente dalla Carta o attratti dall'art. 2 Cost.) si pone il dubbio della scelta tra essi avendo come criteri

1 KANT., *La Metafisica dei costumi*, Roma-Bari, 2009, 348.

2 FEUERBACH, *Principi della filosofia dell'avvenire*, N. Bobbio (a cura di), Torino, 1979, 134.

3 HEIDEGGER, *Essere e tempo. L'essenza del fondamento*, P. Chiodi (a cura di), Torino, 1978, 161.

4 LÉVINAS, *Etica e spirito*, in *Difficile libertà*, G. Penati (a cura di), Brescia, 1986, 56 - 62.

5 RODOTÀ, *Quattro paradigmi per l'identità*, in *Nuova giur. Comm.*, Suppl. al fasc. 4, 2007, 21. Il testo, senza note, è oggi pubblicato anche in Rodotà S., *Il diritto di avere diritti*, Roma-Bari, 2012, 298.

6 DONATI, *Sociologia delle relazioni*, Bologna, 2013, 41.

7 DI MAJO, *La tutela civile dei diritti*, 3, Milano, 2001, 93. In particolare, l'A. precisa che "ove la tutela si sostanzi in regole di proprietà, è il segno che l'ordinamento ha di mira la protezione di un assetto distributivo già dato e che si vogliono già a priori scoraggiare o contrastare attività o iniziative in contrasto con quell'assetto. Ove invece la tutela si sostanzi in regole di responsabilità i confini saranno più mobili; attività o iniziative, pur lesive dei diritti, sono giuridicamente possibili (anche se illecite) anche se gli autori debbono sopportarne i costi e ciò in termini di risarcimento dei danni versus i titolari di diritti o portatori di interessi".

di riferimento i principi di necessità, sufficienza e proporzionalità; se, viceversa, il conflitto avviene tra interessi di rango diversi, prevale il superiore sull'inferiore[8].

Nel caso che ci occupa, cioè il rapporto tra prerogative della persona e Intelligenza Artificiale, la soluzione del conflitto può trovare appigli nelle esperienze riconducibili agli ulteriori diritti esaminati, cioè all'immagine, all'identità, alla riservatezza e all'oblio. Tuttavia, l'indagine resta scivolosa se sufficientemente non si inquadra lo spazio di gara. Si gioca, difatti, in un campo metafisico, aereo, intangibile, in una sorta di iperuranio algoritmico in cui, come si vedrà in seguito, si è assistito già in tema di Internet ad una deresponsabilizzazione dei gestori e al perseguimento (per lo più cieco) di superiori principi di *neutralità* volti, nel paradossale intento di agognare ad una libertà totale di informazione, a non frapporre nel tragitto dei 'pacchetti' dei dati alcun controllo o limite d'accesso e d'uscita[9], quindi alcun presupposto causale ad un ipotetico giudizio di responsabilità.

1. Il prisma dell'identità nella vita di relazione.

Ne 'La cifra' Borges ebbe a scrivere "Nello specchio c'è un altro che spia". L'alterità dello sguardo ben può spiegare il fenomeno attuale della cd. moltiplicazione dell'identità: si può *essere* un'unica persona, ma *apparire* in infiniti modi. E tale moltiplicazione ben può confliggere con gli interessi dei terzi. Per meglio intendersi, nel 1982-1983, su un sistema di *forum* statunitense denominato *CompuServe*, un 'riservato' psichiatra cinquantenne di *New York* di nome Alex si spacciò per un'altezzosa ed antireligiosa donna muta divenuta anche paraplegica in seguito ad un incidente stradale: il *nick name* era Joan. L'impostura, messa in atto per "*meglio relazionarsi con le sue pazienti*", andò avanti per circa due anni nei quali Joan (*rectius*: Alex) diventò un personaggio pubblico, costruendosi un'identità alquanto dettagliata e una fitta rete di relazioni. La messinscena, terminata quando Joan coinvolse un amico conosciuto *on line* in un incontro con Alex (dunque, con un sé medesimo sdoppiato), provocò sconforto e conseguenze negative nei partecipanti al *forum*[10].

Nell'attuale sistema 'liquido'[11], l'identità è sempre più una "costruzione continua"[12]: è il susseguirsi di vicende personali, esperienze di vita, modelli di pensiero, inclinazioni, atteggiamenti, dati genetici, dati informatici a volte plurimi che, sommandosi nel tempo, delineano i tratti dell'individuo, lo fotografano verso gli altri, a volte imprigionandolo. Non si tratta, quindi, di ridurre più l'ambito di discussione alla sola qualificazione giuridica dell'identità[13], bensì di vagliare i possibili contorni del problema, le sfumature, le molteplici sfaccettature, la simultanea compresenza di più personalità, l'interesse degli altri ad una mia identificazione certa nelle trattative commerciali, l'obbligo dell'io di mostrarsi, il suo diritto a scomparire e così via. In breve, non più una, ma molteplici identità, quasi a voler condividere l'impostazione, solo a prima vista provocatoria, di un'accorta dottrina[14] la quale ha avuto

8 MORRONE, *Bilanciamento (giustizia costituzionale)*, in *Enc. dir.*, Annali II, Tomo II, Milano, 2008, 185.

9 Sul principio di neutralità, con riferimento ad Internet, RUOTOLO, *Internet (Dir. Internazionale)*, in *Enc. dir.*, Annali, VII, 2014, Milano, 545. Con riferimento alla I.A., SANTOSUOSSO, *Intelligenza artificiale e diritto. Perchè le tecnologie di IA sono una grande opportunità per il diritto*, Milano, 2020, 16.

10 In http://it.wikipedia.org/wiki/Fake (consultato il 15/05/2020).

11 Il riferimento è a BAUMAN, in *La società individualizzata. Come cambia la nostra esperienza*, Roma-Bari, 2002, nonchè ID., *Modernità liquida*, Roma-Bari, 2003 e ID., *Vita liquida*, Roma-Bari, 2006.

12 RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. critica dir. priv.*, 1997, 583.

13 Per un'analisi generale del diritto all'identità, BAVETTA, *Identità (diritto alla)*, in *Enc. dir.*, XIX, Milano, 1970, 953; CERRI, *Identità personale*, in *Enc. giur.*, XV, Roma, 1989, 1; ZENO ZENCOVICH, *Identità personale*, in *Digesto* civ., Torino, 1993, 294; PINO, *L'identità personale*, in AA.VV., *Gli interessi protetti nella responsabilità civile*, vol. II, Torino, 2005, 367- 394; ZATTI, *Dimensioni ed aspetti dell'identità nel diritto privato attuale*, in *Nuova giur. comm.*, Suppl. fasc. 4, 2007, 1; FINOCCHIARO, *Identità personale (diritto alla)*, in *Digesto civ.*, Agg., Torino, 2010, 721.

14 LOMBARDI VALLAURI, *Identità, identificazioni*, in *Nuova giur. comm.*, Suppl. al fasc. 4, 2007, 11.

modo di "inventariare" almeno quattordici identità personali a seconda dell'angolo visuale di riferimento. Rilevano, per tal verso, svariate facce di un unico prisma[15], tra cui i dati genetici, anagrafici, storici, politici, sessuali, informatici, medici e così via, ognuno dei quali importanti nella *proiezione sociale*. L'identità, difatti, non è una mera identità soggettiva, cioè non riassume ciò che io ritengo di me medesimo, ma è l'oggettivizzazione dei miei dati personali verso l'esterno, la sintesi che di tali dati risalta verso gli altri nella mediazione sociale: l'identità personale non esiste senza mediazione sociale. Essa è in quanto i dati personali - sia soggettivi (opinioni, idee), che oggettivi (immagine, nome) - vengano proiettati dall'io verso l'esterno. Ed in tal senso continuano ad essere condivisibili le parole utilizzate nel lontano 1985 dalla Cassazione nel noto caso Veronesi[16] laddove i giudici di legittimità posero l'accento sulla "vita di relazione".

Il rapporto mediato, allora, impone alla discussione due problematiche assordanti soprattutto alla luce della novella identità digitale: da un lato la libertà (o meno) dell'io di rappresentarsi verso l'esterno in modo assoluto ed incondizionato e dall'altro il diritto (o meno) dell'altro ad utilizzare senza limiti i dati identitari dell'io[17].

La problematica è di più agevole soluzione nel secondo caso ove la giurisprudenza si è attestata sulla possibilità di utilizzare (o riutilizzare) i dati acquisiti sulla rete, ma *storicizzandoli* o, meglio, *contestualizzandoli*[18]. Tali attività vanno eseguite non dal gestore del motore di ricerca, bensì dal titolare del sito nella cui memoria il dato è inserito e conservato. Il titolare dovrà operare nell'osservanza dei criteri di proporzionalità, necessità, pertinenza e non eccedenza allo scopo. La contestualizzazione, per qualche verso, mitiga (ma non supera) la diversa problematica del diritto all'oblio su Internet, problematica che meglio sarà analizzata in seguito.

Più complessa è, invece, la questione dell'utilizzo *sine limine* da parte dell'io dei propri dati identitari. Il distacco dalla fisicità comporta la possibilità di moltiplicarsi con, a volte, abusi identitari che creano problematiche non tanto per il proprietario del dato, bensì per gli altri che col primo vengono a contatto. E' vero da un lato che va "garantita la possibilità di una vita sullo schermo che si esprima attraverso la scelta di assumere identità diverse, di

15 Di prisma parla FINOCCHIARO, *op. cit.*, 723.

16 Con la sentenza n. 3769 del 22 giugno 1985, gli Ermellini ebbero a precisare che l'identità personale era "l'interesse del soggetto, ritenuto generalmente meritevole di tutela giuridica, di essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale o particolare, è conosciuta o poteva essere riconosciuta con l'esplicazione dei criteri della normale diligenza e della buona fede oggettiva". La decisione è pubblicata in *Dir. inf. e informatica*, 1985, 965, con nota di FIGONE.

17 Il conflitto tra 'io' ed 'altro' si pone anche rispetto all'identità genetica che meriterebbe altra e più approfondita indagine. Sul punto, le norme di riferimento possono essere individuate nell'art. 90, primo comma, del D.lg. 196/2003 che subordinava il trattamento dei dati genetici al previo consenso da parte del Garante della Privacy (articolo oggi sostituito dall'art. 27, comma 1, lettera b) del D.Lgs. n. 101/2018 che ha dato applicazione al Regolamento EU n. 279/2016) e nell'art. 12 della Convenzione sui diritti dell'uomo e la biomedicina firmata ad Oviedo che limita i test predittivi. Rilevanti sono anche gli artt. 21 della Carta dei diritti fondamentali dell'Unione Europea e 11 della citata Convenzione di Oviedo. Sul tema, v. RODOTÀ., *La vita e le regole, tra diritto e non diritto*, Milano, 2006, 177.

18 In tal senso, la Corte di Cassazione, nella nota sentenza n. 5525 del 5 aprile 2012 (in *Dir. inf. e informatica*, 2012, 452, con nota di FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, 383), ha precisato che "il soggetto cui l'informazione oggetto di trattamento si riferisce ha in particolare diritto al rispetto della propria identità personale o morale, a non vedere cioè 'travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale' (...), e pertanto alla verità della propria immagine nel momento storico attuale". Ciò implica, continua la Corte, la necessità di "garantire la contestualizzazione e l'aggiornamento della notizia già di cronaca", dunque di aggiornare gli archivi informatici, tenuto conto della memoria 'piatta' di Internet. Cfr. anche RESTA, *Identità personale e identità digitale*, in *Dir. inf. e informatica*, 2007, 511.

presentarsi ad altri con un molteplice corpo virtuale"[19], ma è anche vero che, nel doveroso bilanciamento di interessi, vanno tutelati anche quelli esterni tra cui l'affidamento dei terzi e ciò soprattutto nelle cd. trattative contrattuali. Come già evidenziato da una dottrina[20], non pare sussistente un generale obbligo di rivelare agli altri la propria identità e ciò anche sulla falsariga di strumenti civilistici già disciplinati dal codice quali la rappresentanza indiretta[21] o di fattispecie contrattuali nelle quali la rilevanza dell'identità è stata minimizzata o, addirittura, esclusa[22]. Ne deriva che il nodo centrale si sposta dall'identità all'identificazione e, poi, da questa all'adempimento: ove l'esecuzione della controprestazione venga adeguatamente garantita, la modalità attraverso cui l'individuo si rappresenta non appare più così rilevante. Sul punto è da precisare che oramai l'esigenza di verificare l'identità dell'utente ha trovato riscontri tramite varie applicazioni sempre più perfezionate tra cui l'indirizzo IP, i *cookie*, i servizi di *cloud*, a cui poi si sono aggiunte le frequenti richieste di credenziali d'accesso, la verificazione o la autenticazione tramite chiavi unidirezionali. Tutte modalità di controllo che hanno reso certa per i terzi non solo la individuazione del processore da cui si opera, ma via via anche chi esegua l'operazione, oltre a cosa si desideri e, addirittura, da dove l'utente stia operando[23]. Cosa diversa è, poi, l'adempimento che solitamente nelle transazioni telematica è immediato o garantito da strumenti di pagamento alternativi. E', dunque, possibile concludere nel senso che il potere dell'io di disporre dell'identità personale sia accordabile in via generale anche nei casi più articolati purché, in ossequio al generale principio di buona fede, vengano garantite la identificazione del soggetto e l'esecuzione della prestazione, dunque il corretto adempimento[24].

2. L'immagine di sé.

La questione è regolata dall'art. 10 c.c., titolato 'abuso dell'immagine altrui'[25], e dagli art. 96, 97 e 98 della legge sul diritto d'autore[26].

---

19 RODOTÀ, *op. ult. cit.*, 30.

20 AFFERNI, *L'obbligo di rivelare la propria identità durante una trattativa*, in *Nuona giur. comm.*, Suppl. fasc. 4, 2007, 81.

21 Alla quale può aggiungersi la società fiduciaria.

22 BIANCA, *Diritto civile, 3, il contratto*, Milano, 1998, 59. L'A. Fa riferimento ad esempio "alle vendite mediante macchine a distribuzione automatica" per le quali aggiunge che "in questi contratti l'identità non è influente ai fini della conclusione del contratto (contratti a soggetto indifferente), e l'identificazione può rendersi necessaria al solo fine di accertare l'avente diritto alla prestazione principale o alla prestazione di garanzia. A tale scopo può anche essere sufficiente l'identificazione mediante contrassegni di legittimazione (scontrini, biglietti, ecc.)".

23 Sulla identificazione cfr. QUARTA e SMORTO, *Diritto privato dei mercati digitali*, Milano, 2020, 55 ss., nonché RESTA, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Dir. inf. e informatica*, 2014, n. 2, 171.

24 Certezze che, d'altronde, ben potranno o potrebbero col tempo raggiungersi per il tramite del *blockchain*. Rispetto ai dati personali, v. GAMBINO e BOMPREZZI, Blochchain *e protezione dei dati personali*, in *Dir. inf. e informatica*, 2019, 619.

25 Il quale dispone che "qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni".

26 L. 22 aprile 1941 n° 633 (in G.U. 16/07/1941). E' da precisare che la legge sul diritto d'autore è di data anteriore all'entrata in vigore del Codice civile. Il dettato dell'art. 10 c.c. ricalca, in parte, quello di cui all'art. 97, secondo comma, L. 633 e, difatti, nella Relazione del Ministro Guardasigilli al Codice Civile che il diritto all'immagine "è già disciplinato dalla legge 22 aprile 1941, n. 633, sulla protezione del diritto di autore (articoli 96 e 97), ma non poteva nella parte del codice civile, relativa ai diritti della personalità, mancare una norma che affermasse il diritto sul proprio ritratto. E' da rilevare che la disposizione del codice integra la disciplina della legge speciale, poiché concede l'azione a tutela del diritto all'immagine in due ipotesi distinte: nel caso in cui l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei limiti

La spiccata attitudine patrimoniale del diritto all'immagine[27] postula per assodato il potere in capo all'io di disporre non del proprio diritto (personalissimo e inalienabile), bensì dell'esercizio dello stesso[28]. Ne vanno, tuttavia, esaminati i limiti e se essi siano solo volti verso l'esterno o anche l'interno, cioè se essi debbano applicarsi solo agli altri o anche all'io. Tale problematica va, però, circoscritta rispetto all'oggetto, poichè una cosa è la propria immagine, cioè il proprio ritratto, altra è la propria persona o, meglio, il proprio corpo. La prima è regolata dall'art. 10 c.c., il secondo dall'art. 5 c.c., norme che in taluni casi (si pensi a quelli in cui tali beni sono dall'io o dagli altri utilizzati come veri e propri strumenti di consumo: ne siano esempi il settore pornografico o quello dei c.d. *reality show*) possono entrare in contrasto tra loro. Di là, ad ogni modo, dai giudizi morali, il bilanciamento tra libera disponibilità e reputazione, tra autoregolamentazione e onore, tra paternalismo e decoro è, in questi casi, davvero complesso29.

La dottrina si è mossa su due fronti contrapposti, il primo permissivista fondato sulla "coscienza sociale"30, il secondo, più accorto alla "gerarchia dei valori prefigurata dalla vigente Costituzione"31 e, dunque, avversa ad un deificazione del consenso. La problematica non appare di semplice soluzione: un'impostazione restrittiva, oltre che irrealistica, potrebbe apparire contraria alle odierne teorie liberali, laddove un eccessivo permissivismo comporterebbe (ed ha, invero, già comportato) il travalicamento di valori un tempo indiscussi. Il punto sta, allora, nel valutare se l'interesse tutelato dall'art. 10 c.c. abbia o meno valenza pubblicistica, cioè se onore, reputazione e decoro corrispondano alla dignità umana, al buon costume e all'ordine pubblico. Non è questa la sede per dilungarsi su tali concetti32. Basti, tuttavia, dire che salta evidente all'occhio la diversa terminologia utilizzata dal legislatore nei suindicati artt. 10 e 5 c.c. E', difatti, noto che quest'ultimo ritiene illegittimi gli atti di disposizione del corpo "contrari alla legge, all'ordine pubblico o al buon costume"; la stessa dizione non è ripetuta nell'art. 10 il quale contempla differenti valori. Salvo, allora, a voler ritenere errato il linguaggio del legislatore, deve concludersi per una diversa scala di valori, la lesione dei quali non comporta i medesimi effetti: il proprio ritratto, in breve, non ha il medesimo peso specifico del proprio corpo. E', dunque, necessario valutare quando la lesione dell'onore, della reputazione o del decoro possa ingenerare anche lesione della dignità umana. In mancanza, la violazione dei valori indicati dall'art. 10 c.c. non potrà di per sé comportare alcun effetto negativo in presenza del consenso del titolare dell'immagine. L'io, dunque non potrà disporre della propria immagine soltanto laddove l'atto di disposizione procuri lesioni anche ai principi generali di buon costume e ordine pubblico[33].

---

stabiliti dalla legge speciale, e nel caso in cui l'esposizione o la pubblicazione avvenga con offesa al decoro o alla riputazione della persona ritrattata".

27 Al punto da essere definito "diritto *nuancé*, inerente alla persona, ma al contempo suscettibile di assumere una marcata valenza patrimoniale": in tal senso, RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, 144, il quale precisa che il termine *nuancé* è di ZACCARIA, *Diritti extrapatrimoniali e successione. Dall'unità al pluralismo nelle successioni a causa di morte*, Padova, 1988, 35-36.

28 Sul potere di disposizione del diritto all'immagine, GIUFFRIDA, *Il diritto all'immagine*, in *Il diritto privato nella giurisprudenza* a cura di Cendon P.*, Le persone, III, Diritti della personalità*, Torino, 2000, 203.

29 In tal senso, URCIUOLI, *Autonomia negoziale e diritto all'immagine*, Salerno, 2000, 186.

30 BIANCA, *Diritto civile, 1, La norma giuridica, i soggetti*, Milano, 2002, 186. Nello stesso senso, appare orientato GIUFFRIDA, *op. cit.*, 45. Nello stesso senso si è mossa una giurisprudenza: Trib. Roma, 7 ottobre 1988, in *Giust. civ.*, 1989, I, 1243 e in *Dir. inf. e infomatica*, 1989, 173, con nota di SCOGNAMIGLIO, *Richiami di dottrina e giurisprudenza.*

31 SCOGNAMIGLIO, *op. cit.*, 179.

32 Per un approfondimento, v. ANSALONE, *Il diritto all'immagine*, in Nuova giur. comm., 1990, II, 227 e TRABUCCHI, *Buon costume*, in *Enc. dir.*, V, Milano, 1959, 700.

33 In tal senso può leggersi la Delibera n. 23/07/CSP resa in data 22 febbraio 2007 dall'Autorità per le Telecomunicazioni, in forza della quale si è limitata la distribuzione da parte delle emittenti radiotelevisive

Nel bilanciamento degli interessi contrapposti, in particolare a presidio del diritto dell'altro, non vanno, però, dimenticate le deroghe stabilite dal primo comma dell'art. 97 l.d.a. Il consenso della persona ritratta non è necessario "quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico". In tali casi, prevale l'altro sull'io poiché si tende a tutelare "l'interesse preminente della collettività a conoscere l'immagine di quelle persone (...)"34. Il consenso del titolare dell'immagine non è necessario, dunque l'immagine potrà rendersi pubblica anche in sua assenza.

Tra tali eccezioni spicca la *notorietà* della persona celebre che è stata, da parte di una dottrina, intesa come ulteriore diritto oltre il medesimo diritto all'immagine[35]. Si tratterebbe, in particolare, della prerogativa da parte del personaggio celebre di trarre profitto dalla propria immagine anche laddove per la sua pubblicazione non fosse necessario il suo consenso. Di là dalla qualificazione giuridica, ciò che comunque emerge è che, per il caso di notorietà, si assiste ad un limite doppio agli interessi contrapposti: se, difatti, l'io non può opporre la mancanza del proprio consenso alla (legittima) pubblicazione della sua immagine, l'altro non potrà trarne profitto esclusivo: si tratta, dunque, di un'eccezione all'eccezione che dà luogo ad un necessario contemperamento tra poteri di auto ed eterodisposizione.

3. Riservatezza ed *accountability*.

Il bilanciamento degli interessi informa di sè l'intera materia del trattamento o, meglio, della *circolazione* dei dati personali[36]. Il Reg. UE 2016/679 (anche noto come *General Data Protection Regulation* o GDPR)[37] ha novellato, abrogandola, la Direttiva 95/46/CE ed ha prodotto notevoli modifiche nelle disposizioni nazionali europee.

Partiamo da due punti. La normativa in questione è, anzitutto, "onnipervasiva"[38]: ai sensi

---

pubbliche e private, nazionali o locali, di trasmissione di programmi contenenti scene pornografiche. Tale Delibera è stata assunta a seguito di due interessanti precedenti giurisdizionali e precisamente Cass., Sez. I, 6 aprile 2004 n. 6759 (in *Dir. inf. e informatica*, 2004, 433) e Cass., Sez. I., 6 aprile 2004 n. 6760 (in *Dir. famiglia*, 2004, 703).

34 BAVETTA, *Immagine (diritto alla)*, in *Enc. dir.*, XX, Milano, 1970, 144. Nello stesso senso, ANSALONE, *op. cit.*, 235.

35 Sul punto, v. SCOGNAMIGLIO, *Il diritto all'utilizzazione economica del nome e dell'immagine delle persone celebri*, *Dir. inf. e informatica*, 1988, 1; MARCHEGIANI, *Il diritto sulla propria notorietà*, in *Riv. dir. civ.*, 2001, I, 191. Tra le tante decisioni, cfr. Pret. Roma, 14 febbraio 1986, in *Giust. civ.*, I, 1987, 2418, con nota di DOGLIOTTI, *Ancora sul diritto all'immagine di personaggio noto*, nonché Cass., 12 marzo 1997 n. 2223, in *Dir. inf.* E INFORMATICA, 1997, 544, con nota di RESTA, *<<Così è (se vi ap-pare)>>: identificabilità della persona celebre e sfruttamento economico della notorietà*. Interessante è anche la nota di commento di RESTA alla delibera dell'Autorità Garante della Concorrenza e del Mercato del 31 ottobre 1996, in *Nuova giur. comm.*, 1997, I, 713, dal titolo *Il c.d. diritto all'utilizzazione economica dell'immagine tra autonomia negoziale e diritto della concorrenza*.

36 Già prima del GDPR l'Autorità Garante della privacy si era mossa nel senso del bilanciamento degli interessi. In tal senso, v. "Reti telematiche e Internet - Motori di ricerca e provvedimenti di Autorità indipendenti: le misure necessarie a garantire il c.d. diritto all´oblio" (https://www.garanteprivacy.it/web/guest/home/doc-web/-/docweb-display/docweb/1116068 - consultato il 5 giugno 2020), nonché "Archivi storici on line dei quotidiani: accoglimento dell´opposizione dell´interessato alla reperibilità delle proprie generalità attraverso i motori di ricerca - 11 dicembre 2008" (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1582866 - consultato il 5 giugno 2020), nonché "Provvedimento a seguito di richieste di cancellazione, dai risultati resi da un motore di ricerca, dei collegamenti alle pagine web che contengono il nominativo dell´interessato - 16 aprile 2015" (https://www.garanteprivacy.it/web/guest/home/doc-web/-/docweb-display/docweb/4006473 - consultato il 5 giugno 2020).

37 Recepito in Italia dal D.Lg. 10 agosto 2018 n. 101 (in G.U. Serie Generale n. 205 del 4 settembre 2018).

38 L'aggettivo è usato da FINOCCHIARO, *Il principio di accountability*, in *Giur. it.*, 2019, 2778.

dell'art. 4, n. 2, del Reg., il trattamento è, difatti, "*qualsiasi* operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali"; inoltre, sempre l'art. 4, ma al n. 1, precisa che i dati personali consistono in "*qualsiasi* informazione riguardante una persona fisica identificata o identificabile («interessato»)". La onnipervasività va intesa anche dal punto di vista personale (il considerando n. 14 estende la protezione a tutte le persone fisiche "*a prescindere* dalla nazionalità e dal luogo di residenza") e territoriale (i considerando 22 e 24 estendono l'applicabilità del Reg. "*indipendentemente* dal fatto che l'attività di trattamento avvenga all'interno dell'Unione" ed anche quando il trattamento venga eseguito "ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito nell'Unione"). In secondo luogo, il principio di bilanciamento è presente, oltre che nel corpo delle norme, anche nei medesimi considerando. Nel quarto, in particolare, si stabilisce che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità"[39]. Enunciazione questa assolutamente rilevante poiché tesa a contemperare diversi concetti *pesanti*, tra cui la 'funzione sociale' (che nell'ordinamento italiano ha assunto un ruolo determinante nella teoria sulle limitazioni al diritto di proprietà[40]) e la necessità del contemperamento, utilizzando il contrappeso della proporzionalità. Ancora, nel considerando 69 si legge che "è opportuno che incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato".

Il bilanciamento (tra l'io e l'altro) va analizzato avendo riguardo tanto all'oggetto della discussione (cioè ai dati), quanto ai protagonisti del trattamento e ai rispettivi poteri o, meglio, prerogative. Per iniziare, basti dire che dall'analisi complessiva del Regolamento il rapporto tra oggetto e soggetto, meglio tra dati e consenso, pende enormemente in favore dei primi i quali sono intesi dallo stesso legislatore europeo come beni di scambio utilizzati, a causa della rapidità dell'evoluzione tecnologica, tanto dalle imprese private quanto dalle autorità pubbliche nello svolgimento delle loro attività: si predilige, in breve, "la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali" (considerando 6)[41].

In questo quadro, il consenso dell'interessato, sebbene religiosamente richiamato ai considerando 32, 42 e 43[42], è poi relegato a condizione di liceità del trattamento nella *sola* lett. a) dell'art. 6 e, si badi bene, alternativamente alle altre cinque ipotesi di cui al medesimo art. 6. Tale scelta è stata, presumibilmente, operata dal legislatore europeo per tre ragioni: la prima è dare oramai atto dell'imprescindibile rilevanza economica dei dati personali nell'ambito delle attività istituzionali e commerciali; la seconda è prendere finalmente nota della fumosità,

39 Il 'considerando' continua in un'elencazione dei diritti fondamentali, delle libertà e dei principi riconosciuti dalla Carta e sanciti dai trattati, in particolare "della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica".

40 Sul punto, v. RESCIGNO, *Proprietà (dir. priv.)*, in *Enc. dir.*, XXXVII, Milano, 1988, 254 (in part. 271).

41 Il punto è posto in evidenza da POLETTI, in *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, 2783.

42 La religiosità, invero fittizia, è presidiata dalle prerogative in favore dell'interessato, in particolare dal diritto di informazione (art. 12), di rettifica (art. 16), di limitazione del trattamento dei dati (art. 18), di portabilità dei dati (art. 20), di opposizione (art. 21) ed, infine, di cancellazione dei dati, ovverosia il diritto all'oblio (art. 17). Tutti tali diritti subiscono molteplici eccezioni che danno adito di sospettare sul reale peso del consenso in tema di privacy. Per un'analisi dei vari diritti contemplati nel reg., PIRAINO, *I 'diritti dell'interessato' nel Regolamento generale sulla protezione dei dati personali*, in *Giur. it.*, 2019, 2789.

in molte pratiche contrattuali, del rilascio del consenso da parte dell'interessato; infine la terza è spostare il peso del dato personale dall'interessato (che doveva rincorrere) al titolare (che deve ora provare l'adozione di una serie di misure appropriate). Nel procedimento di bilanciamento, dunque, il Regolamento si preoccupa di elencare le ipotesi di liceità del trattamento in assenza del consenso e sono quelle di *necessità* dettate dalle lett. b), c), d), e) ed f) dell'art. 6: il trattamento sarà quindi illecito ove le finalità a cui l'utilizzo dei dati servivano potevano essere raggiunte *aliunde*. La necessità dovrà sussistere anche nel procedimento di riutilizzazione dei dati già raccolti e conservati (art. 6, comma 4) e dovrà in ogni caso essere provata dal titolare secondo quanto disposto dal comma 2 dell'art. 5 che stigmatizza il principio di "responsabilizzazione". In ciò consiste la cd. *accountability*, cioè l'obbligo in capo al titolare anzitutto di predisporre un modello organizzativo proporzionale all'utilizzo, ma soprattutto di provare l'adozione delle misure obbligatorie: in tal senso l'art. 24 stabilisce che "il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento", con ciò da un lato rendendo autonomo il titolare in ordine alle misure utili, ma dall'altro responsabilizzandolo in ordine all'*onus probandi*. Si assiste, in breve, ad una vera e propria inversione dell'onere probatorio che, nel diritto italiano, ha luogo in relazione alle cd. attività pericolose (art. 2050 c.c.) e, in generale, ai casi di responsabilità oggettiva[43], ipotesi senza dubbio estensibile anche al trattamento dei dati personali.

Nel bilanciamento tra l'io e l'altro sorge, tuttavia, il dubbio della tutela laddove si verifichi non il semplice utilizzo dei miei dati ad opera di altri, bensì la diversa ipotesi del *conferimento* da parte mia dei dati personali ad altri, cioè la negoziazione (*rectius*: vendita) da parte dell'utente dei propri dati verso la controprestazione di un servizio reso dal titolare[44]. In questo caso, poco prima dell'entrata in vigore in Italia del GDPR, la Cassazione, con sentenza n. 17278/2018[45], ha puntualizzato che il consenso doveva essere libero, specifico e reso in relazione ad un trattamento chiaramente determinato. Rilevante è stato che i Giudici di legittimità hanno legato la libertà alla fungibilità della controprestazione, precisando che "il condizionamento non possa sempre e comunque essere dato per scontato e debba invece essere tanto più ritenuto sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato". Tale assunto è stato dalla Corte postulato facendo leva sul provvedimento n. 27432 del 29 novembre 2018 dell'AGCM, nonchè sulla lettura dell'art. 7, comma 4, del Reg. UE 679 ancorchè non ancora entrato in vigore alla data della sentenza[46].

Infine, in un'analisi complessiva del bilanciamento di interessi assume rilevanza il diritto dell'interessato alla cancellazione dei dati, ovverosia il diritto all'oblio[47]. L'art. 17 del Reg., in

43 Sia consentito il rinvio a CICORIA, *Quale danno in materia di privacy?*, in *Giust. civ.*, 2007, 39.

44 Sul punto, cfr. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impr.*, 2019, 34.

45 Pubblicata in *Giur. it*, 2019, n. 3, 533, con nota di THOBANI, *Operazioni di* tying *e libertà del consenso*, nonché in *Corriere giur.*, 2018, n. 11, 1459, con nota di CARBONE, *Consenso al trattamento dei dati personali e newsletter promozionali*, nonché in *Nuova giur. comm*, 2018, n. 12, 1775, con nota di ZANOVELLO, *Consenso libero e specifico alle e-mail promozionali*.

46 Tale assunto è stato dalla Corte postulato facendo leva sul provvedimento n. 27432 del 29 novembre 2018 dell'AGCM, nonché sulla lettura dell'art. 7, comma 4, del reg. UE 679 ancorchè all'epoca non ancora entrato in vigore. Per puntualità, l'art. 7, al comma 4, stabilisce che "nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".

47 Sul diritto all'oblio, v. *Il diritto all'oblio su internet dopo la sentenza Google Spain*, a cura di RESTA e ZENO-ZENCOVICH, Roma, 2015, passim; nonché, FINOCCHIARO, *Il diritto all'oblio rispetto ai diritti della personalità*, in *Dir.*

una formulazione nuova rispetto alla Direttiva 95/46/CE, accorda una tale prerogativa, ma a determinate condizioni e comunque ove non sussistano le eccezioni di cui al terzo comma[48]. Si tratta di una serie di ipotesi a tal punto pregnanti da, per la verità, sminuire enormemente il potere dell'interessato, ridimensionandolo ad una sorta di diritto condizionato o, peggio, ad un barlume di diritto. Ne deriva che, da un'analisi dei presupposti e delle eccezioni fissate dal legislatore europeo, l'ago della bilancia penda, in materia di riservatezza, in favore dell'altro, non dell'io.

4. La AI di terza generazione e il *White Paper* del Parlamento Europeo.

Non v'è un concetto univoco e trasversale di AI[49]. Piuttosto, esistono tentativi di concettualizzazione: la tendenza cioè a fissare parametri, confini o limiti oltre i quali si resta nella intelligenza umana (UI) o si travalica in altre branche del sapere. Tra essi quello che risalta più agli occhi è e resta l'assenza, nelle macchine intelligenti, di vita in senso biologico. In breve, partendo da Alan Turing, passando per la riunione di Dartmouth del 1956, per il *machine learning,* sino ai *Big Data* o all' *Internet of Things*, quello che maggiormente colpisce è che tali macchine non sono *generate naturalmente*, ma sono e resteranno frutto del lavoro dell'uomo o dell'operato di altre macchine intelligenti. Tale differenza (che è cosa ben diversa dalla diade 'intelligenza umana' - 'intelligenza artificiale') deve segnare il *limen* di riferimento che comporta o, meglio, impone, nel rapporto di affiancamento delle macchine intelligenti all'essere umano, una doverosa subordinazione - anche in termini di diritti, prerogative, priorità, responsabilità e quant'altro - delle prime rispetto al secondo[50].

E' inopportuno in questa sede soffermarsi sui concetti di algoritmo, *coding*, reti neurali e

---

inf. e informatica, 2014, 591; nonché sia consentito il rinvio a CICORIA, *Del tempo e della colpa, ovverosia note critiche intorno all'oblio*, in *Foro nap.*, 2016, 3.

48 Il diritto alla cancellazione non si applica nel caso in cui il trattamento sia necessario "a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria". Circa il bilanciamento in tema di oblio, si veda anche prima della novella europea, FINOCCHIARO, *op. ult. cit.*, 603. Da ultimo, rilevanza hanno assunto le decisioni della Corte Europea dei diritti dell'uomo del 24 settembre 2019 ed, in particolare, la Sentenza nella causa C-507/17 (in cui si è stabilito che il gestore di un motore di ricerca non è tenuto a effettuare la deindicizzazione in tutte le versioni del suo motore di ricerca, ma è tuttavia tenuto ad effettuarla nelle versioni di tale motore di ricerca corrispondenti a tutti gli Stati membri e ad attuare misure che scoraggino gli utenti di Internet dall'avere accesso, a partire da uno degli Stati membri, ai link di cui trattasi contenuti nelle versioni extra UE di detto motore) e la Sentenza nella causa C-136/17 (in cui si precisa che il divieto di trattare determinate categorie di dati personali sensibili si applica anche ai gestori di motori di ricerca e che, nell'ambito di una domanda di deindicizzazione, dev'essere effettuato un bilanciamento tra i diritti fondamentali del richiedente la deindicizzazione e quelli degli utenti di Internet potenzialmente interessati a tali informazioni). Entrambe le decisioni sono consultabili in http://curia.europa.eu/juris/documents.jsf?num=C-136/17# (28/05/2020)

49 Sui concetti di AI e sul percorso storico compiuto, v. QUARTA e SMORTO, *op. cit.*, 1-27; nonché, da ultimo CINGOLANI e ANDRESCIANI, *Robots, macchine intelligenti e sistemi autonomi: analisi della situazione e delle prospettive*, in *Diritto e intelligenza artificiale, Profili generali - Soggetti - Contratti - Responsabilità civile - Diritto bancario e finanziario - Processo civile*, a cura di Alpa, Pisa, 2020, 23.

50 E' da discutere se tale rapporto di subordinazione debba essere esteso anche tra la intelligenza artificiale e gli animali (sul punto, v. FOSSÀ, *Frammenti di oggettività e soggettività animale: tempi maturi per una metamorfosi del* pet *da bene (di consumo) a* tertium genus *tra* res *e* personae *?*, in *Contratto e impresa*, 2020, n. 1, 527) e tra la intelligenza artificiale e l'ambiente.

così via[51]. Quello che, viceversa, rileva è che la AI, attraversando una prima fase caratterizzata dalla sequenziazione univoca degli algoritmi e una seconda caratterizzata dall'apprendimento automatico da esperienze pregresse, è giunta ad una terza fase in cui le macchine intelligenti stanno iniziando ad elaborare, dunque ad intrecciare i *Big Data*, ed a eseguire autonomamente ragionamenti di tipo trasversale. La strada percorsa è tanto lunga quanto veloce, nel senso che la velocità operativa con cui si sta evolvendo la AI (così come gli investimenti stanziati da quasi tutti gli Stati[52]) non è proporzionata al tempo trascorso. Ciò, da ultimo, ha obbligato il Parlamento Europeo a dettare alla Commissione talune raccomandazioni in tema di robotica[53] tra le quali enorme rumore ha fatto il disposto di cui alla lett. f) dell'art. 59 col quale si è ipotizzata la "personalità elettronica dei robot"[54].

Di là dal riferimento (invero suggestivo) al mostro di Frankestein di cui al considerando A, appaiono rilevanti talune premesse tra le quali qualla secondo cui "è possibile che a lungo termine l'intelligenza artificiale superi la capacità intellettuale umana". Tale ipotesi (che per la verità è un'evidenza, tenuto conto della velocità di lavorazione dei dati da parte dei robot) reca sconforto laddove non temperata o per qualche verso limitata dal legislatore europeo e, poi, da quello nazionale. Il settore di cui si discute è infatti intimamente collegato al mercato[55], dunque a facili processi di *commodification*. In tal senso, è da notare che i principi generali a cui la Commissione è invitata ad attenersi con riferimento alle caratteristiche di un robot intelligente sono cinque e nessuno di essi fa riferimento al dato dell'eterodirezione. Al contrario, si pone l'accento sull'autonomia, sull'autoapprendimento e sull'adattamento all'ambiente, dunque su requisiti che conducono alla libertà piena o semivigilata. Inutile dire, sia chiaro, che il medesimo Parlamento Europeo ha dettato, nella Risoluzione, una serie di principi etici tra cui spiccano il riferimento ai diritti sanciti dall'art. 2 del Trattato sull'Unione Europea e dalla Carta dei diritti fondamentali dell'U.E. Inoltre, si fissano taluni presupposti dell'AI tra cui che essa deve mirare ad "integrare le capacità umane e non a sostituirle", così come che gli esseri umani debbano mantenere "in qualsiasi momento il controllo sulle macchine intelligenti". Tuttavia, nella Risoluzione si pone l'accento anche sulla loro *imprevedibilità*, riconducibile all'autonomia di cui si vogliono essere dotate e sulla "forte concentrazione di ricchezza e di potere nelle mani di una minoranza" che sarebbe l'ovvia conseguenza collegata allo sviluppo della robotica. In tali gangli si pone il dubbio del

51 Per un'analisi accurata del tema, v. QUARTA e SMORTO, *op. cit.*, 14 ss.

52 Sul punto, l'11 febbraio 2019 il Presidente USA Trump ha firmato l'*Executive Order on Maintaining American Leadership in Artificial Intelligence* le cui linee guida sono consultabili in https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/ (consultato il 30 maggio 2020). La Cina, già nel gennaio 2018 aveva stanziato 2,1 miliardi di dollari per la costruzione in cinque anni di un campus nel quartiere periferico di Mentougou, a ovest di Pechino, di circa 54,87 ettari, con 400 imprese nei settori dei Big data ad alta velocità, cloud computing, biometria, deep learning e internet mobile 5G (https://www.ilsole24ore.com/art/cina-21-miliardi-d-investimenti-il-parco-dell-intelligenza-artificiale-AEcub4bD – consultato il 30 maggio 2020).

53 Risoluzione del Parlamento Europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)). Sulla Risoluzione, v. RODI, *Gli interventi dell'Unione europea in materia di intelligenza artificiale e robotica: problemi e prospettive*, in *Diritto e intelligenza artificiale*, *op. cit.*, 187.

54 L'articolo, in particolare, invita la Commissione ad esplorare, esaminare e valutare le implicazioni di tutte le soluzioni giuridiche possibili su vari temi tra cui "l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi". Sul punto, SANTOSUOSSO, *op. cit.*, 198, nonché CAROCCIA, SOGGETTIVITÀ GIURIDICA DEI ROBOT ?, in *Diritto e intelligenza artificiale*, *op. cit.*, 213.

55 Da ultimo, si leggano le considerazioni in "*Le registrazioni via* blockchain *conquistano il sistema bancario*" di P. Sol., in *Sole 24 Ore*, 27 maggio 2020, 20.

contemperamento dei contrapposti diritti.

5. Il bilanciamento degli interessi nella AI.

Il primo quesito da porsi è chi nell'*Artificial Intelligence* rivesta la posizione dell'*altro*. E' evidente, difatti, che l'alterità in questo settore si può sdoppiare o, addirittura, triplicare e ciò soprattutto se, in un prossimo futuro, si intenda concedere una qualche forma di personalità o soggettività alle macchine intelligenti[56], oltre alle quali è e resta *altro* colui il quale gestisce tali macchine. In tale ultima accezione vi rientrano sicuramente i soggetti coinvolti nello sviluppo e nella commercializzazione di applicazioni dell'intelligenza artificiale ed i soggetti *finali* che tali tecnologie utilizzano, ivi compresa la Pubblica Amministrazione.

Volendo fare qualche esempio, la AI sta ponendo rilevanti problemi in due settori specifici e cioè nel riconoscimento delle immagini, dunque nel campo della cd. *sorveglianza sociale,* e nel settore dell'automazione dei veicoli. Entrambi i settori sono richiamati dalla Risoluzione del 16 febbraio 2017[57] e sono, a tacer d'altro, già presenti nella vita di tutti i giorni: si pensi al cd. *park assist* o al *lane assist* o, ancora, al *cruise control* nelle autovetture e ai sistemi di video analisi nelle videocamere di sorveglianza. In entrambi i casi si pone un problema di responsabilità per i danni arrecati e, quindi, di comprensione del centro di imputazione d'interessi. Per le autovetture l'analisi è stata condotta con accortezza già negli Stati Uniti, giungendo tuttavia a soluzioni, via via che l'automazione aumenta, poco condivisibili poiché sbilanciate in favore del produttore (altro). In particolare, nei veicoli di livello 4 e 5[58], cioè nei veicoli in cui non v'è necessità della presenza del conducente, si è precisato che "la conformità di un veicolo agli *standard* federali delineati dalla NHTSA costituisce un limite oltre il quale non è configurabile una responsabilità civile in capo al produttore che abbia immesso sul mercato un veicolo conforme"[59]. La conformità agli standart eliminerebbe la responsabilità o, in breve, sterilizzerebbe la qualifica de l'*altro*, poiché in dette autovetture non esiste un conducente (e potenzialmente neanche un proprietario, bensì e per il caso di locazione soltanto un produttore). Tale scelta, a fermarsi all'attuale normativa in tema di responsabilità da circolazione stradale[60], lascerebbe con poca o senza tutela, civile e penale, il danneggiato,

---

56 Il punto è esaminato da BERTI SUMAN, *Intelligenza artificiale e soggettività giuridica: quali diritti (e doveri) dei robot ?,* in *Diritto e intelligenza artificiale*, *op. cit.*, 251.

57 L'ultimo sotto agli artt. da 24 a 29, il primo agli artt. 20 e 21.

58 I livelli di automazione sono indicati dalla SAE International (https://www.sae.org/), un ente di normazione nel campo aerospaziale, automobilistico e veicolistico. Dal livello 0, che designa l'auto tradizionale con conduzione interamente umana, si passa al livello 1 (in cui attualmente siamo) con dispositivi ormai diffusi e automatizzati per singole operazioni di guida e ad un alquanto prossimo livello 2 con dispositivi automatici di sterzata, accelerazione e decelerazione in scenari predeterminati. Il successivo livello 3, ancora in fase di sperimentazione, consente l'esecuzione automatica di ogni attività di guida in *mapped environment*, ma impone il monitoraggio del pilota, laddove il successivo e non più avveniristico livello 4 richiede la presenza del pilota solo e soltanto per il caso in cui la guida automatica è resa impossibile da condizioni avverse. Infine, il livello 5 di automazione vede completa autonomia, dunque inesistenza di volante e pedali.

59 AL MUREDEN, Autonomous cars *e responsabilità civile tra disciplina vigente e prospettive* de iure condendo, in *Contr. Imp.*, 2019, n. 3, p. 895. Sulla problematica della responsabilità, cfr. anche Gaeta M.C., *Automazione e responsabilità civile automobilistica*, in *Resp. civ. e prev.*, 2016 n. 5, 1717; nonché PELLEGATTA, *Automazione nel settore* automotive*: profili di responsabilità civile*, in *Contratto e impresa*, 2019, n. 4, 1418; nonché ULISSI, *I profili di responsabilità della macchina dell'apprendimento nell'interazione con l'utente*, in *Diritto e intelligenza artificiale*, *op. cit.*, 435 e CAPILLI, *I criteri di interpretazione delle responsabilità*, in *Diritto e intelligenza artificiale*, *op. cit.*, 457.

60 La problematica è affrontata, con larghe note di rinvio, da GAETA, in *Automazione e responsabilità civile automobilistica*, in *Resp. civ. e prev.*, 2016, 5, 1718 e ss. In particolare, l'A. sottolinea come "la produzione di automobili dotate di elevata tecnologia impone l'introduzione di una specifica normativa per regolamentare eventuali forme di responsabilità civile extracontrattuale da circolazione stradale legata ai nuovi automatismi. Infatti, le norme esistenti non affrontano direttamente il problema della responsabilità in caso di collisioni automobilistiche che coinvolgono un veicolo autonomo o, quantomeno, semiautonomo" (p. 1723). La

laddove l'altro (in questo caso il produttore) sarebbe, in un bilanciamento di interessi, eccessivamente agevolato. La problematica, tutt'altro che teorica, andrebbe regolata nel breve periodo e ciò in vista dell'incedere velocissimo della materia[61]. Medesime questioni, seppur con le dovute differenze, nascono nel settore della videosorveglianza. Società extra UE ipotizzano di potere a breve analizzare i *terabyte* di dati in *streaming* dalle telecamere a circuito chiuso nelle aree pubbliche. In tal modo, si potrebbe, attraverso il procedimento del riconoscimento facciale di microespressioni, migliorare la sicurezza nelle strade cittadine, alle fermate degli autobus o nelle stazioni ferroviarie[62]. Tale modello di sicurezza - attuabile mediante l'incrocio di videocamere, droni e satelliti e già in parte utilizzato da talune forze dell'ordine - imporrebbe delle evidenti restrizioni alla *privacy* di ciascuno, con probabilità, in incerta percentuale, di errori di Lombrosiana memoria. Anche in tal caso è da porsi il quesito di chi sia l'altro, apparendo un po' riduttivo il costrutto che tende a deificare la macchina, rendendola 'persona' responsabile. Nè ad idea diversa può giungersi attraverso una equiparazione della macchina alla 'persona giuridica' [63] (seppure di Kelseniana memoria), laddove quest'ultima ha organi propri di gestione e di controllo, oltre a rapporti giuridici, cosa che non è ipotizzabile facilmente per una videocamera o un sistema di *cruise control*. E', dunque, necessario sancire un principio di responsabilità, preferibilmente oggettiva per i risvolti probatori, che dia certezza dell'imputazione giuridica, cioè di chi sia l'altro64.

Ulteriore problematica poi è quali siano gli interessi contrapposti e, quindi, da bilanciare. Poichè l'*io* ha necessità di godere di una maggiore sicurezza e protezione, ma ha parimenti necessità di non essere derubato dall'*altro* di ogni proprio singolo dato, movimento, espressione, pensiero e così via. Dal canto suo, mentre l'*altro* ha l'interesse, prevalentemente economico, a produrre l'automatismo perfetto o la razionalizzazione delle spese di

---

problematica è stata parzialmente affrontata, ma con residue ombre soprattutto in materia penale, dal d.m Trasporti del 28 febbraio 2018 (ma sul punto, v. nt. 61). Della stessa A. e più recente, cfr. *Liability rules and self-driving cars: the evolution of tort law in the light of new technologies*, Napoli, 2019, passim. Si vedano anche le considerazioni di GATT, MONTANARI, CAGGIANO, *Consent to the processing of personal data: a legal and behavioural analysis. Some Insights into the Effectiveness of Data Protection Law*, in *European Journal of Privacy Law & Technologies On line journal*, Torino, 2018/1, 1; nonché GATT, CAGGIANO, GAETA, *Italian Tort Law and Self-Driving Cars: State of the Art and Open Issues,* in AA.VV. (a cura di) Oppermann e Stender - Vorwachs, *Autonomes Fahren. Technische Grundlagen, Rechtsprobleme*, Rechtsfolgen, 2019, 239; nonché, *Per un'Intelligenza Articiale antropocentrica. Intervista a Lucilla Gatt*, in https://www.dimt.it/news/intel-ligenza-artificiale-antropocentrica/ (consultato il 27 ottobre 2020).

61 Si veda l'articolo comparso su *Sole 24 Ore* del 28 maggio 2020, p. 21, dal titolo "*Amazon pronta a salire sul* robo-taxi zoox". E' da precisare che in Italia la materia è regolata ancora a livello di d.m. In particolare, l'art. 19 del d.m. Trasporti del 28 febbraio 2018, recante 'Modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di Smart Road e di guida connessa e automatica' (in G.U. Serie Generale n. 90 del 18 aprile 2018), stabilisce che "il richiedente deve dimostrare di avere concluso il contratto di assicurazione per responsabilità civile specifica per il veicolo a guida automatica, ai sensi della l. 24 dicembre 1969, n. 990, depositando una copia presso il soggetto autorizzante, con un massimale minimo pari a quattro volte quello previsto per il veicolo utilizzato per la sperimentazione nella sua versione priva delle tecnologie di guida automatica, secondo la normativa vigente". Il contratto di assicurazione deve indica espressamente che l'assicuratore è a conoscenza delle modalità di uso del veicolo e che il veicolo è utilizzato in modalità operativa automatica su strade pubbliche.

62 Si leggano le considerazioni in *Così Intelligenza Artificiale e videosorveglianza potrebbero mettere in pericolo libertà e privacy*, in https://www.lastampa.it/topnews/tempi-moderni/2019/06/28/news/cosi-intelligenzaartificia-le-e-videosorveglianza-potrebbero-mettere-in-pericolo-liberta-e-privacy-1.36544531 (consultato il 6 giugno 2020).

63 In senso contrario, SANTOSUOSSO, *op. cit.*, 203 ss.

64 Spunti di riflessione possono leggersi in FRATTARI, *Robotica e responsabilità da algoritmo. Il processo di produzione dell'intelligenza artificiale*, in *Contratto e impresa*, 2020, n. 1, 458; nonché COMANDÈ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giur. Econ.*, 2019, n. 1, 169.

produzione, l'*io* ha il contrapposto interesse a godere della massima sicurezza per il caso di danno. Il discorso si complica ulteriormente se, agli interessi privati, si aggiungono, prevaricandoli, gli interessi pubblici, come ad esempio l'interesse alla sicurezza o l'interesse alla salute o all'ambiente. Interessi, invero, che provocherebbero dei deragliamenti rilevanti o quanto meno dei cambiamenti di traiettoria, poiché i diritti fondamentali - quelli cioè che vengono richiamati (invero a volte per ragioni tutte solo esornative) dalle varie Carte, Convenzioni internazionali o Direttive - sono esclusivamente miei e non certo altrui.

Conclusions.

Al *White Paper* del Parlamento Europeo ha fatto seguito la Comunicazione della Commissione europea al medesimo Parlamento, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, titolata "Creare fiducia nell'intelligenza artificiale antropocentrica"[65]. In essa si fissano i principi basilari cui attenersi: intervento e sorveglianza umani, robustezza tecnica e sicurezza, riservatezza e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale, *accountability*. Tra essi due potrebbero apparire per qualche verso interessanti, cioè l'*accountability*, così muovendosi la Commissione nel solco della normativa sulla riservatezza, e il benessere ambientale, schiudendosi dunque lo sguardo anche sul dato ecologico. Tuttavia, è bene dire che, di là dalle enunciazioni di principi e dal richiamo al dato dell'etica, si legge di tempi futuri: di ciò che si farà, di ciò che si dirà. Ma è tardi.

Dall'analisi, per così dire, comparata degli altri diritti della personalità appare pressocchè complesso ricavare una qualche regola che possa alleviare il problema del bilanciamento degli interessi confliggenti nella AI: disponiamo di strumenti *vecchi* e soprattutto tremendamente *lenti*. I richiamati diritti fondamentali appaiono sempre più spesso delle *scatole vuote* e ciò soprattutto perchè la regola fissata dai vari legislatori è che essi possono essere continuamente derogati: prova ne sia la sorte recente che ha avuto il consenso rispetto alla necessità nel GDPR. Stessa cosa è a dirsi per l'oblio rispetto alle proprie immagini, ai dati e all'identità, oblio che è consentibile solo e soltanto a determinare condizioni e che, oramai, appare annacquato dai principi questa volta giurisprudenziali della contestualizzazione e della storicizzazione. E' inevitabile concludere che, via via che si procede lungo la strada della storia umana, si assiste ad un allargamento dell'interesse dell'*altro* rispetto all'interesse dell'*io*, quasi a voler stigmatizzare il ripudio per l'egoismo contro il vittorioso incedere dell'altruismo[66]. Il punto è che tale avanzata se in un primo momento ha avuto luogo tramite istituti quali la "funzione sociale" che ha avuto il merito di contemperare il mio terribile diritto[67] con le esigenze superindividuali di matrice sociale, allo stato si legge di superamento della AI rispetto alla UI, di necessità di controllo, di sorveglianza sociale, di macchine intelligenti imprevedibili, di autonomia gestionale, di concentrazione di potere e ricchezza nelle mani di una minoranza[68]. Tutti rischi, sia chiaro, che possono e forse devono essere

65 Comunicazione dell'8 aprile 2019, in https://ec.europa.eu/transparency/regdoc/rep/1/2019/IT/COM-2019-168-F1-IT-MAIN-PART-1.PDF (consultato il 30 maggio 2020).

66 Sulla diade egoismo-altruismo in sociologia, DURKHEIM, *Dizionario delle Idee*, *La sociologia tra riflessione metodologica e impegno etico-politico* (a cura di) Mariano, Roma, 1998, 3.

67 Faccio riferimento al saggio di RODOTÀ, *Il terribile diritto, Studi sulla proprietà privata e i beni comuni*, Roma, 1990, passim.

68 Non possono ad esempio tacersi gli effetti collaterali riconducibili all'utilizzo da parte di una politica di *machine learning* volta, sfruttando gli *hastag* che ritiene opportuni, a sensibilizzare la platea elettorale in un verso o nell'altro. In tal senso, v. Cresce il consenso di Salvini sui social? Ecco cosa ha capito l'intelligenza artificiale, in *Sole 24 Ore*, 5 settembre 2018 (https://www.infodata.ilsole24ore.com/2018/09/05/cresce-consenso-salvini-sui-social-cosa-capito-lintelligenza-artificiale/ - consultato il 5 giugno 2020).

corsi laddove si constati che la AI possa aiutare il comparto medico e della sanità in generale o ridurre il dispendio delle energie combustibili nella costruzione dei beni di consumo. Ma qual è il costo da pagare ? Nella problematica - invero seccante ed oramai anacronistica - del bilanciamento degli interessi, la Commissione UE nella citata Comunicazione, al punto 2.3, parla di una 'Prossima tappa' "che coinvolga il più ampliamente possibile i *portatori di interessi*". Tuttavia se ci si domanda chi siano tali portatori, può trovarsi un'amara risposta all'interno della stessa Comunicazione laddove al punto 1 si legge che "per attuare tale agenda strategica comune di ricerca, innovazione e diffusione dell'IA, la Commissione ha intensificato il dialogo con tutti i pertinenti portatori di interessi dell'industria, degli istituti di ricerca e delle autorità pubbliche". Nella speranza che tali portatori rechino con sé anche l'interesse dell'io, cioè quello del singolo cittadino che, per le più svariate ragioni condivisibili o meno, non abbia intenzione di partecipare in via assoluta a questo processo di *liquidazione* dell'io, sia consentito ricordare che gli strumenti di cui si serve il giurista sono e devono restare strumenti *filosofici*[69], dunque distanti da quelli solo economici che sembrano informare di sé l'attuale evoluzione dell'AI e ciò a presidio di un orientamento da ripudiare, cioè di una tendenza alla *commodification* in ogni settore umano. Dati allora tali strumenti, l'AI potrà assurgere ad opportunità e non demone da abiurare soltanto laddove si fissino taluni paletti imprescindibili e che bilancino realmente due interessi contrapposti: da un lato la costante e crescente tendenza ad una globalizzazione in ogni dove del sapere umano (che reca con sé una falsa democratizzazione orizzontale), dall'altro il presidio di ciò che di meno globalizzato esiste e cioè i diritti fondamentali (che recano con sé una reale democratizzazione verticale)[70].

Tra tali paletti ci si permette di indicare: la comprensione della macchina (dunque il diritto di ciascuno di poter cogliere l'algoritmo che ha prodotto un determinato risultato), la strumentalità della macchina rispetto all'uomo, alla natura e agli animali (dunque il ripudio dell'autonomia della macchina o di ciò che non è naturalmente generato), infine il diritto dell'io di estromettere la macchina dalla mia - e solo mia - sfera privata (dunque l'abdicazione dell'interesse altrui ad entrare, spiandolo, nel mio focolare domestico). Qualcosa di nuovo? No, al contrario: soltanto paletti che già appaiono da altri discussi e ben approfonditi, ma che finanche nelle Comunicazioni o nelle Risoluzioni testé analizzate sembrano, per così dire, sfumati, poco ricalcati nei tratti distintivi, in breve postposti o quanto meno parificati ai differenti interessi di carattere mercatorio.

69 In tal senso, IRTI, *Nichilismo Giuridico*, Roma-Bari, 2005, VII. Spunti di riflessioni sul tema possono leggersi in CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi Giur. Econ.*, 2019, n. 1, 47.

70 La contrapposizione tra macchina e diritti umani è posta in rilievo da LIMONE, *L'algoritmo e il mondo della vita, Nuovi appunti sul fondamentalismo macchinico nell'era contemporanea*, in *Persona, periodico internazionale di studi e dibattito*, 2017, n.1-2, 1.

SECTION II
FOCUS PAPERS

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Child protection on social networks in the era of Covid-19 confinement

VALERIA MANZO
Ph.D. (c) at University of Campania Luigi Vanvitelli
Lawyer in Naples

Abstract

While it is true that in the digital age minors have considerable tools to express their personality and exercise the rights recognised by international conventions (also through the use of technologies that allow new models of relationships), the continuous process of renewing applications inevitably results in a greater concentration of information with consequent exposure to greater risks for security and privacy.

In this context, due to the confinement measures caused by the COVID-19 pandemic emergency, children have become even more dependent on social media in order to stay in touch with their friends, to express their feelings, to study and to distract themselves.

The aim of this survey is to address the specific issue of children's interactions on social media and the impact in terms of privacy and data protection as their vulnerability has further increased in the light of the confinement emergency.

Keywords: Minors - social media - social networks - privacy - data protection - GDPR - COVID-19 - TWIGIS.it - Jonathan Galindo.

Summary: 1. The relationship between minors and social media. – 2. The protection of minors in the GDPR. – 3. Digital awareness. – 3.1 The TWIGIS.it platform. – 4. Social media in the COVID-19 era - The Jonathan Galindo case. – Conclusions.

1. The relationship between minors and social media.

The advent of social media has brought about a revolution in the ways of interaction and personal communication, which has had a profound impact on relational activities and a greater concentration of information with relative exposure to higher risks for the security and privacy of users.

Although living in a constantly evolving technological framework, some widespread processes can be identified that constitute the identifying traits of the social media[1] phenomenon.

In a study conducted in 2015[2] these were the four common characteristics identified:

--- the use of Web 2.0[3];

[1] R. Cafari Panico, *From Internet to Social Media*, (1nd edn, Maggioli 2013).

[2] J.A. Obar, S. Wildman, 'Social Media Definition and the Governance Challenge: An Introduction to the Special Issue' (2015) Telecommunications Policy, vol. 39, n. 9, 745-750.

[3] Web 2.0 means the phase of the Web following Web 1.0, characterised by the possibility for users to interact and modify the contents of the web pages of a site, portal or web platform.

--- the absorption of User-Generated Content (UGC)[4];
--- profiling users of the site or app;
--- the connection of profiles with those of other users or user groups.

If you do a Google search by writing "minors and social media" as first results you will see a series of articles and insights indicating the "risks" they run and a series of instructions for parents to protect and defend them.

For the digital natives, the net is not "one of the many means of communication", but "the main dimension of life" with the consequence that the relationships woven online, the sharing on social networks and the perception of the world increasingly mediated, impose new needs for protection, in the face of the inadequacy of the traditional categories of the law to regulate phenomena in continuous evolution.

As a vehicle of opportunities for growth and emancipation, the web risks, if lived in the absence of the necessary awareness, to expose increasingly fragile children to underestimated dangers, on the side between illusion of autonomy and introjection of rules and exercise of responsibility[5].

To give an example, these are the most frequent dangers:

--- sharing and dissemination of personal information and photographs;
--- violent content;
--- distortion of reality;
--- addiction;
--- use of the data for commercial purposes with consequent advertising bombardment;
--- social isolation[6].

Well, by catalyzing social media attention to phenomena such as those just mentioned, can it be considered that they are not the cause?

Starting from the children's sense of responsibility that inevitably passes for their parents, the problem must be placed in today's social and educational context where young people all too often find themselves facing the age-old problem of growth, even within a digital context, alone or in the company of false teachers.

Among the factors capable of positively influencing the awareness of minors, the role of teachers[7] and parents[8] remains fundamental, as well as the emulation of positive behaviour[9]. In particular, parents should be familiar with social tools and learn how to use them in order

---

[4] UGC, i.e. user-generated content, means any type of content made accessible through social platforms such as blog posts, wiki contributions, forum discussions, tweets and podcasts.

[5] Hearing of the President of the Guarantor for the protection of personal data, Antonello Soro, follow-up to the cognitive survey on forms of violence among children and against children and adolescents - Parliamentary Committee on Children and Adolescents (8 July 2020) on https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9434094.

[6] S. Weeden, B. Cooke & M. McVey, 'Underage Children and Social Networking' (2013) Journal of Research on Technology in Education, vol. 45, n. 3, 249-262.

[7] K. Davis, C. James, 'Tweens' Conceptions of Privacy Online: Implications for Educators' (2013) Learning, Media and Technology, vol. 38, n. 1, 4-25.

[8] S. Yusuf, M. Nizam Osman, M. Salleh, H. Hassan, M. Teimoury, 'Parents' Influence on Children's On-line Usage' (2014) Procedia - Social and Behavioral Sciences, vol. 155, 81-86; S. Livingstone, K. Ólafsson, E. J. Hel-Sperd, 'Maximizing Opportunities and Minimizing Risks for Children Online: The Role of Digital Skills in Emerging Strategies of Parental Mediation' (2017) Journal of Communication, vol. 67, n. 1, 82-105.

[9] Y. Seounmi, 'Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk- Benefit Appraisal Approach' (2005) Journal of Broadcasting & Electronic Media, vol.49, n. 1, 86-110.

to encourage children to use them consciously and, at the same time, monitor their online activities[10].
The "neutrality" of the web, understood as susceptibility to harmful or solidarity-based uses, charges users with responsibility for their online conduct and makes adults responsible for the delicate task of making children aware of how extraordinary, but also risky, the new dimension of life can be.
Rather than talking about the need to save children from social media, it should be about helping them to cope with growth problems by providing them with answers they can confront and learn to live the digital spaces available to them.
As the Council of Europe's Guidelines on the Rights of the Child in the Digital Environment underline, a real education, ethical and civic digital literacy would be the tool to enable children to draw all its extraordinary resources from the web in order to be "digital aware citizens".

2. The protection of minors in the GDPR.

Although *datafication* and connectivity simplify daily activities, the regulatory framework for the protection of minors, however articulated, does not seem sufficiently protective[11].
To counteract the vulnerability of data subjects, EU law grants them specific individual rights including the right to be informed of the fact that their data is being collected, the right of access to retained data, the right to object to unlawful processing and the right to rectification, erasure and blocking of data.
The Data Protection Directive requires that data subjects consent to data processing, regardless of the sensitivity of the data being processed (see Articles 7, 8 and 14).
A child-friendly consent procedure implies that the child's developing capacities are taken into account and, therefore, his or her progressive involvement.
The first step requires that the child's legal representative consults with the data subject before authorizing the processing; then, consent must be obtained from both the legal representative and the child; finally, consent is required only from the child when the latter is an adolescent[12].
In order to define the "risk" phenomenon it is necessary to recall the notion of *networked self* (i.e. the virtual projection of one's own identity) and identify the perception of minors themselves with respect to the threats connected to the use of social media.
The prolonged use of digital instruments that convey personal data, often without control, can well generate exponential risks that also involve the psychic-cognitive development of the child who does not yet have a fully trained understanding capacity[13].
From this point of view, among the negative effects of the so-called *privacy paradox*, as documented in the sociological literature, there is the tendency for the most fragile subjects

[10] According to the Wall Street Journal, Facebook is studying a technology to "link" children's profiles to those of their parents so that they can authorize their children's friendships and applications to use.
[11] D. Lupton, B.Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' (2017) New Media & Society, vol. 19, n. 5, 780-794.
[12] FRA, *Handbook on European Law relating to the rights of the child* (2015).

[13] These include online communication with unknown subjects; exposure to content promoting anorexia, self-harm, drug use or suicide; cyberbullying; images of injuries to other children and exchange of sexual images.

to underestimate the dangers in terms of privacy and to underuse the tools made available[14]. While Directive no. 46 of 1995[15] made no distinction between the processing of children's and adults' data, as a consequence of the risk-based approach, the GDPR has taken a central role, having understood the protection of children's privacy as "data minimisation and computerisation".

Article 8 of Regulation (EU) 2016/679 specifically provides: "*Where Article 6(1)(a) ("when the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes") applies, with regard to the direct provision of information society services to minors, the processing of the child's personal data is lawful when the child is at least 16 years of age. Where the child is under 16 years of age, such processing shall be lawful only if and to the extent that such consent is given or authorised by the holder of parental responsibility.*

Member States may establish by law a lower age for these purposes provided that it is not less than 13 years old.

The data controller shall make every reasonable effort to verify in such cases that consent is given or authorised by the holder of parental responsibility for the child, in view of the technologies available.

Paragraph 1 shall be without prejudice to the general provisions of the contract law of the Member States, such as the rules on the validity, formation or effectiveness of a contract in relation to a minor".

The division made by the rule between the limits and conditions of the *privacy* consent and the contractual consent raises the following questions:

--- the minor could validly stipulate a contract and be "sub-threshold" for the provision of consent to the processing of data;

--- i.e. he could independently provide *privacy* consent without being able to validly enter into a contract, with the consequence that, in the first case, a valid contract (inasmuch as it complies with the requirements of personal development) will be opposed to unlawful data processing; while in the second case, a valid provision of consent for the lawfulness of the processing will be opposed to the cancellation of the contract itself[16].

When talking about children's "digital" rights, it should not be overlooked that access to web services is not only a right to exercise other rights (freedom to search, receive and disseminate information and ideas, to freely express one's opinion in terms of thought, conscience and religion, to associate and come together peacefully) but it is also the means by which certain rights can be protected where there is a real or alleged violation or where there is social discomfort related to the exercise of the child's freedoms.

For this reason, Recital no. 38[17], in stressing the greater risk associated with the processing of personal data of minors, has led to the strengthening of information tools (with a view to

---

[14] *Ex plurimis*, A. Thiene, 'The personality rights of children in virtual space' (2017) Annals online of Teacher Education and Training, vol. 9, n. 13, 26-39; A. Spangaro, *Minors and mass media: old and new means of protection* (1nd edn, Ipsoa, 2011), C. Perlingieri, 'La tutela dei minori di età nei social networks' (2016) Review of Civil Law, n. 4, 1324 et seq.

[15] It was first implemented by Law no. 675/1996 and then by Legislative Decree no. 196/2003.

[16] Childhood and Adolescence Watchdog, Note to the Prime Minister on the need to implement training programmes to develop digital awareness of underage people for digital consent, 10 September 2018 on https://www.garanteinfanzia.org/news/decreto- privacy-14-anni-il-consenso-ai-servizi-web-agia-ora-educazione-alla-consapevolezza.

[17] *According to* which: "*Children deserve specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards involved and their rights with regard to the processing of personal data. This specific protection should, in particular, cover the use of children's personal data for marketing purposes or the creation of personality or user profiles and the collection of personal data relating to children when using services provided directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of prevention or counselling services provided directly to a child*".

forming a conscious consent), as well as to the provision of rules for processing built as an objective imposed on the owner made responsible for the adoption of specific technical rules that achieve the protection of personal data.
According to a study on the cognitive development of minors conducted by the Stanford Children's Health paediatric centre, the typical phases in the growth of a child/adolescent were highlighted[18].
If between 6 and 12 years of age, we find the phase of the so-called concrete cognitive development, relative to the ability to think and reason, carrying out concrete operations on objects and actions, between 12 and 18 years of age, instead, the so-called complex thought develops, characterized by formal logical operations that allow the child to think about different possibilities, to reason from known information, to consider different points of view debating ideas and opinions, until reaching autonomous and personal decisions.
Sticking to the purely "medical-scientific" approach, the child, already at the age of 13, is in the midst of developing his or her personal identity and, therefore, normally "capable of discernment" also with regard to the use of information society services.
Although a child is "capable of discernment", can we share the concern of the European legislator when trying to make the web safer?

3. Digital awareness.

While increasing the minimum age of validity of consent, it can certainly not prevent access to "harmful" content circulating on the web.
In fact, to consider the issue resolved after preventing access to digital services means to reason in the abstract, denying a phenomenon.
On the occasion of the XIII Safer Internet Day 2017, the Safer Internet Day set up and promoted by the European Commission, the Blue Telephone has organised a special event at the Chamber of Deputies, an event entitled "The relationship between young people and the internet" in which a survey carried out by Doxa Kids was presented as a preview. The survey showed that, in Italy, among the under 13 respondents (out of a sample of over 600 adolescents) 73% habitually use WhatsApp, 44% Facebook, 35% Instagram, 13% Snapchat and 11% Twitter.
This data clearly shows how digital natives are able to circumvent the limitations of the network to create profiles or accounts even in the 9-12 age group.
If, therefore, the problem seems to be the non-existence of a training programme included in education that educates children to use digital technologies safely, preventing them from accessing information society services would only generate a greater sense of curiosity.
On balance, keeping the age of autonomous digital consent high would not help to prevent risks if the rise was not accompanied by appropriate training of those to whom consent is given.
But is it realistic to think that these measures are a form of protection for children?
A recent study carried out by EU Kids Online[19], which coordinates and stimulates surveys on how children use new media, with particular reference to risks and web security measures, said that the more children use the Internet, the more they acquire digital skills and are able to seize opportunities on the Internet, comparing content and websites and assessing the

[18] On https://www.stanfordchildrens.org/en/topic/default?id=cognitive-development-90-P01594.

[19] On http://eprints.lse.ac.uk/60512/1/EU%20Kids%20onlinie%20III%20.pdf.

reliability of information.
Education in the use of digital platforms is not, however, the only aspect to be considered in terms of learning, as there is also education through digital platforms.
During her speech in New York on July 12, 2013, in the UN Headquarters, Malala Yousafzai, the youngest Nobel Peace Prize winner because of her commitment to the affirmation of civil rights and the right to education, was asked: "What would you recommend to someone who believes that an injustice is happening in her community but who does not know how to start making a real impact to remove it?
Such is the answer: "I think it's easy. It's full of people who would start wondering 'Who do I have to meet to say what's going on? Where do I have to go to do it? '. But the tool in front of you is social media. Use them. [...] It is difficult to stand up and tell a Taliban that what they are doing is wrong if they are in front of you in your house. It is easier to start a peaceful protest on Facebook".
Well, teaching is also applicable to children's use of social media and web services: not everyone is in a position to ask their parents for consent, not everyone would get it, yet often the first step to remove physical and mental injustice is to create a social profile or to join a virtual space where they can express their opinion freely and without parental interference in their personal sphere. After all, privacy is also this.

3.1 The TWIGIS.it portal.

If in the beginning there were the late digital immigrants (who grew up without technology and were sceptical about its use), digital immigrants (born in an analogue world but adapted to use technology) and digital natives (who from birth have had to deal with technology), today the eyes are focused on the "mobile- born" or children who, even before learning to walk, already know how to move easily on PCs, smartphones and tablets[20]
Paul Holland, general partner at the Foundation Capital, wondered what the "mobile-born", once grown up, expect from technology.
According to Holland, their approach to furniture will force them to rethink ways and timescales of the traditional day in the office, including new interfaces, software and hardware to be refurbished; assuming that offices, as we know them today, will still exist.
Whether it is work or leisure, the key word will be interactivity, since, according to the "mobile-born", everything can be implemented with software.
At the moment, the curiosity of children for tablets and the like represents a new challenge, especially for companies.
If Intel has acquired Kno, a startup specialising in the construction of educational software whose flagship product is interactive textbooks to browse on mobile, Facebook, along with other big names, from Google to Yale University, in Panorama Education, a startup that uses online surveys to collect data that will then be processed and used to improve the school environment, trying to solve problems such as bullying.
There are also those who, like the Israeli startup Twigis, have tried to create child-proof versions of tools already used by adults, launching a social network and an information portal for children between 6 and 12 years of age which, while safeguarding their privacy, provides a space in which they can develop their creativity and share experiences.
On Twigis:

[20] According to a Common Sense Media study conducted in the USA, if the percentage of two-year-olds using a mobile device is 38%, this rises to 63% in children under the age of eight.

--- minors have a personalized profile on which they cannot post pictures but only create avatars;
--- it is necessary to insert the email of your parents, who will have to give their consent;
--- all content and messages are screened in advance by a group of moderators in an anti-bullying manner that provides for the suspension (from two days to one month) from the social if one user targets another[21];
--- personal information is not disclosed, not even through cookies.
The portal consists of two sections: in the news section minors can read articles and comics (for which it is also possible to create new ones to share with the community), as well as follow interactive videos and tutorials aimed at doing DIY jobs; in the games section there is a large collection divided into categories such as adventure, action, sport, board games and cards.
This gives children the opportunity to experience virtual worlds in a safe digital environment that stimulates their skills and creativity.

4. Social media in the COVID-19 era - The Jonathan Galindo case.

While lockdown confinement has forced many children to make further use of social media in order to stay in touch with each other, it has also exposed them to increased vulnerability to violence, abuse and online grooming.
According to the Lanzarote Committee's "Declaration on the Protection of Children from Sexual Exploitation and Sexual Abuse during the COVID-19 Period", adopted on 15 May 2020, it is essential to assess the impact of the pandemic crisis management measures in place and to adapt the responses of child protection systems to the new situation by ensuring that all children are confined to safe environments.
As recently stressed by the Global Partnership to End Violence against Minors and UNICEF, together with partners in the Alliance for the Protection of Children and Adolescents in Humanitarian Action, the prevention of exploitation and abuse and safe reporting of concerns should be an integral part of all COVID-19 prevention and control measures.
In the document, the Committee recalls how the measures taken by States to contain the pandemic have exposed "*children to a greater risk of abuse, neglect, exploitation and violence*".
It reads as *follows:* "As a *result of the confinement measures, children are increasingly online and depend on social media to stay in touch with friends, express feelings, study, distract themselves": a large number of children are therefore likely "to be lured online and become victims of sexual extortion, cyberbullying or other sexual exploitation facilitated by technology*".
For the Committee, therefore, it becomes "of the *utmost importance that helplines and hotlines are known both to minors and to the general public and that they are made available 24 hours a day, including through online platforms*" and that States ensure that they have adequate human resources and equipment so that no request for help is left unanswered.
Attention is also asked for initiatives "*that inform children and young people, in a manner appropriate to their age, of the assistance and support services, both physical and psychological, to which they still have a right of access*" and states are invited to provide forms of support for parents and guardians in the management of children's emotions and behaviour during the crisis situation.

[21] It is no coincidence that important partnerships have been signed in Italy with the Telefono Azzurro and the Moge (Italian parents' movement) who have participated in the analysis and definition of the structure of Twigis.it's contents, in addition to the collaboration of the State Police.

The Council of Europe, for its part, has developed a series of awareness-raising documents focusing not only on the detection and reporting of violence against children, but also on issues such as how to talk to children about COVID-19, how to manage time spent in front of a screen during an emergency, how to assist during confinement and how to ensure online safety at a time of social distancing[22].

The isolation to which minors have been forced in recent months has led some of them to adopt bolder online behaviour, making them even more vulnerable.

On 30 September last, the main Italian newspapers reported the tragic news of an 11-year-old Neapolitan minor who took his own life.

The victim, before killing himself by jumping off the balcony, would send a message WhatsApp to the mother of the following tenor: "*Mommy, Daddy I love you. Now I have to follow the man in the black hood. I am running out of time. Forgive me.*

What is most frightening is the lucidity with which an unavoidable deadline and an appointment with an irreversible death are put off.

The reconstructions carried out led to identify in "Jonathan Galindo" the referee of a deadly online game from the image of an anthropomorphic dog (a sort of Walt Disney's Goofy with a sinister smile) whose objective would be to convince the interlocutor to take part in the so-called "game".

Such is the consolidated dynamic: the referee of the challenge would begin by sending a request for friendship to minors on social networks and then write them a private chat message of the following tenor: "Do you want to play a game?

Any positive response would start a game of tests of courage to the point of self-harm.

But who is hiding behind Galindo? The truth is that anybody can wear his clothes on social networks and it is difficult to think that behind the many profiles created there is only one person hiding.

Through Google Trends it has been possible to observe how the first mentions of this *creepypasta* phenomenon with a terrorist background were made in January 2017, with epicentre in Latin America and India, and how interest in the "Jonathan Galindo" search key began to grow in May 2020, and then exploded in July.

While the deadly challenge on TikTok has become a summer trend (demonstrating the proliferation of videos in which users dance against the background of screens captured from conversations with the one who is supposed to be an occult persuader), on Facebook, Instagram and Twitter profiles there has been a split between users who have raised the alarm[23] and users who, instead, have publicly announced that they want to play the role of the anthropomorphic dog in order to scare their friends.

The question arises, therefore, spontaneously: what motivates minors to accept the challenge?

According to some reconstructions, the victim would be "frightened" by demonstrating to the referee that he knows his location and IP address.

What if it is a spirit of emulation? or a viral phenomenon of fashion"? And above all, why

---

[22] On https://www.coe.int/en/web/children/covid-19.

[23] A tweet from @uh_xsh on July 2nd, which went viral, is a perfect example of how these online dynamics work. The text of the tweet is as follows: *"*WARNING* If you are reading, you are obliged to rewire. Make your friends stay alive. Circulating an account called Jonathan Galindo, they are the masters of the Blue Whale Challenge whose intent is to convince you to commit suicide. If someone sends you a dm ("direct message") or interacts with you, block it".*

do children feel "obliged to continue rehearsing"?
Analysing the elements of the challenge in question, it is easy to see quite a few similarities with other deadly online games developed since 2017; Think of the Blue Whale phenomenon (a 50-day course - coordinated by a tutor - which involves challenges of increasing difficulty aimed at destroying children's self- esteem to the point of convincing them that their life is worth nothing and therefore leading them to suicide), the Tide Pods Challenge (challenge to eat capsules of washing machine detergent), the Bird Box Challenge (challenge to perform actions such as driving blindfolded), the Balconing (challenge to dive from a balcony of a flat or hotel room into a swimming pool only after taking drugs or alcohol), or the Momo Challenge (challenges ranging from watching horror films to self-harm).
The real danger of these "games" is the so-called "Werther effect" (or Copycat suicide), a phenomenon of emulation that leads to an increase in suicides after the news of a suicide published in the media.
How, then, can we combat the phenomena of deadly games online? The World Health Organisation has published a *vademecum* for the press which calls for a "responsible presentation of information" avoiding sensationalism, excessive amplification of the news and details on suicides[24]".
The answer seems, therefore, aimed at containing, as far as possible, the high mediaticity in order to avoid the emergence of new emulative phenomena and the protagonism that, too often, minors hide within themselves.
But can this be considered sufficient? In the writer's opinion, no, because at a time when the network has become an inseparable companion, starting from the fragility and emotional instability of children, it is all too often forgotten how fundamental the active presence of parents is through dialogue (in order to understand whether their children are aware of what Social Challenges actually are and what they entail) and careful monitoring (aimed at noticing suspicious behaviour or bodily injury).

Conclusions.

Never as in the current era have families, schools and civil society been called upon to recognise and share their educational skills and knowledge respectively, in order to enhance the growth of children and strengthen the influence of their role as active citizens, aware adults capable of becoming reference points for future generations[25].
The web is no longer just a virtual place to visit, but an atmosphere that surrounds reality itself, constantly bringing new possibilities and concerns closer together.
Therefore, the challenge for the educational, social and family system becomes the constant updating on the evolution of technologies by spreading the culture of "media education" and educating minors to a responsible and conscious use of the web and social networks without, however, neglecting the non-virtual reality of which they should not be spectators, but actors, becomes an activity of considerable importance.

[24] On https://www.who.int/mental_health/prevention/suicide/resource_media.pdf.
[25] A. Alesina, A. Ichino, *Homemade Italy. Survey on the real wealth of Italians*, (1nd edn, Mondadori 2009).

EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Energy and sustainability between ecology of law, green law and nature rights

PAOLA GRIMALDI
Ph.D. at the University Federico II of Naples
Lawyer

Abstract

The Planet is facing an unprecedented ecological crisis. Renewable energy and energy efficiency are key ingredients to face the challenge of reducing CO_2 production, which is considered a fundamental action to tackle climate disruption. Establishing frameworks of Green economy and Green Law is needed to enable the conversion towards an ecologically sustainable society. The European Union has set up a policy that pushes member states to increase the use of renewable sources and reduce fossil fuels, especially oil and gas. In Italy, with the PNIEC, the national targets for 2030 on energy efficiency, targets of use renewable sources and the reduction of CO_2 emissions are established, as well as the targets for energy security. However, the Italian government needs to design more extensive policies, particularly regarding the subject of eco-adaptation.

Keywords: Energy - Emissions - Green - Economy - Law - Ecology - Sustainability - Nature.

Summary: Introduction. – 1. Green Law in Italy, EU, and the world. – 2. Future perspectives and open problems for a Green Italian legal framework. – Conclusions.

Introduction.

Pollution and climate change are pushing the planet one step away from global ecological disruption. Data emerged from the UN Scientific Committee's Climate Gas Emission Report [1] [1] within the United Nations Environment Program (UNEP) have shown that the temperatures reached an average increase in temperatures just below 1 degree Celsius and that the average increase in temperature would be of 3.2 degrees by the end of the century, even considering the commitments made by different countries up to that moment. This launched the call to multiply efforts and investments to achieve the objectives of the 2015 Paris Agreement [2] [2]. This rise in the global average temperature beyond the recommended threshold would increase the intensity and frequency of the environmental disasters recorded to date (heat waves, drought, famines, floods, melting ice, and so on) as alerted by the Intergovernmental Panel on Climate Change[3]. As recommended by many, therefore, it is necessary to bet on the Green Economy and on the development of a Green Law system that establishes renewable energy solutions and energy efficiency as key ingredients to face the challenge of reducing CO_2.

Green Law in Italy, EU, and the world.

Certain Italian legal doctrine, which for some time has been denouncing the serious

[1] Presented in Geneva on August 8, 2019.
[2] See Climate Action / Paris Agreement on www.ec.europa.eu.
[3] See Special Report "Climate Change and Land" on www.ipcc.ch.

ecological crisis facing Italy, proposes an ecological conversion of the main institutions of the Italian legal system[4], now obsolete in the face of the dramatic environmental situation in our country. For example, these authors formulate an "ecological" analysis of contract law and propose the establishment of a new contractual instrument, called the "ecological contract", implementing a different way of satisfying needs. This new contractual tool is inspired by the need of a more sustainable economy[5]. All accompanied by a necessary "ecological literacy"[6] of individuals to help them reflect on new ownership forms and on the change in the relationship between the sovereign state sphere and the shared global one. In the field of energy and sustainability, virtuous examples of this reflection are some countries of Latin America, where Nature[7] is elevated as a legal subject[8] and protected at the constitutional level. Nine Latin American Countries—Chile, Peru, Ecuador, Costa Rica, Honduras, Guatemala, Haiti, the Dominican Republic and Colombia— have set a new collective energy target for 2030 which consists in the use, at that date, of 70% of renewable energy [REF] through targeted government plans involving use of clean energy sources, smart grids and increased sanctions for fossil fuel emissions.

The European Union has set up a policy that pushes member states to increase the use of renewable sources and reduce fossil fuels[9], especially oil and gas. EU legislation on the promotion of renewable energies has evolved significantly in recent years and the future political framework for the post 2030 period is under discussion[10].

In Italy, the energy regulatory framework has so far been fragmented between different standards and, especially in the field of renewable energies, growth has been slow and not at all competitive[11]. However, on January 21 2020, the Italian Ministry of Economic Development published the Integrated National Plan for Energy and Climate (*Piano Nazionale Integrato Energia e Clima*, PNIEC), which incorporates the changes contained in the Decree Law on Climate[12] as well as those on investments for the Green New Deal envisaged in the Budget Law 2020. The Green New Deal is a government plan to promote urban regeneration, energy conversion towards a widespread use of renewable energies, the protection of biodiversity and seas, the fight against climate change. This name refers to the New Deal, the set of social and economic reforms launched by the President F.D. Roosevelt in the 1930s to lift the United States from the Great Depression. The underlying idea is that this bundle of green policies is born as a response to the current great crisis, the climatic one.

---

[4] For an overview on the point see F Capra, U Mattei, Ecology of law. Science, politics, common goods, (Aboca Edizioni, 2016); U Mattei, A Fourth, Turning point, (Aboca Edizioni, 2018).

[5] M Pennasilico, 'Sustainable development and "ecological contract": another way of satisfying needs'(2016) 4 RDC 1291,1323.

[6] See F Capra, defending the Earth, our common home, beyond the differences of ethnicity, culture or class.

[7] M Carducci, 'Nature (rights of)' [2017] DPD 486, 52.

[8] MC Gaeta, 'Il problema della tutela giuridica della natura: un'analisi comparata tra Italia e stati dell'America latina (2020) 4 Nuova Diritto Civile, 305 ss.; MC Gaeta, 'Principio di solidarietà e tutela di nuovi "soggetti" deboli. La Foresta Amazzonica quale soggetto di diritto (analisi della sentenza n. 4360/2018 della Corte Suprema di Giustizia della Colombia' (2019) Familia, Observatory section of private international law and comparative law, online page of 29 August 2019, Pisa; S Baldin, 'The rights of nature in the constitutions of Ecuador and Bolivia' (2014) 10 Latin-American visions of the Study Center for Latin America 25, 39.

[9] C Benanti, 'Energy labeling as a market regulation tool'[2018] 6 CNLC 1364,1386.

[10] For a detailed reconstruction of the regulatory framework on the topic of renewable energy which was mentioned in the text, cf. www.europarl.europa.eu.

[11] From Law 239/2004 on the reorganization of the energy system to Law 99/2009 on the security of the energy sector to Legislative Decree 387/2003 and Legislative Decree 28/2011 which are accompanied by Legislative Decree 192/2005 and subsequent amendments on energy performance in construction and Legislative Decree 104/2014 on energy efficiency.

[12] DL October 14, 2019, n. 111 converted into Law 12 December 2019, n. 141 on G.U. 292 of 13 December 2019.

In particular, the PNIEC establishes the national targets for 2030 on energy efficiency, renewable sources and the reduction of CO2 emissions, as well as the objectives regarding energy security, the single energy market and competitiveness, development and sustainable mobility. For each of the aforementioned, the PNIEC describes measures that will be implemented to ensure their achievement.

Future perspectives and open problems for a Green Italian legal framework.

In this perspective we offered a reasoned overview of the current challenges regarding climate emergency, energy conversion, and sustainability and presented how Italian policy makers concretely acknowledged this issues with establishing the PNIEC. The hope is that the Italian legislator will now put in place all the necessary and adequate legislative and economic provisions that can pursue the common objectives established at European level.

The Italian legislator should consider five actions to take:

- the recognition of a juridical subjectivity to Nature as a "common good";
- the introduction in the Italian legal system the concept of energy as a common good, instead of a commodity;
- a full and expedite transposition of Directive 2018/2001/ EU on the development of renewable sources, which sets the target of 32% electricity from renewable sources by 2030, indicates the share of RES in transport at 14%, plans to eliminate the use of palm oil, sets the reduction of CO2 emissions to 40%, and includes sustainability criteria for solid biomass;
- to introduce the model of "energy communities", already present in other European countries (Denmark, Holland and Germany), where electricity, strictly generated from renewable sources, is used, sold and shared in smart grids;
- to introduce specific rules in the context of civil liability, and frame them in the context of intergenerational responsibility.

Focusing on the last proposal, Governments should create compulsory civic-environmental education courses in schools that can raise and promote awareness of these issues from an early age. These would consist of training projects aimed at spreading the knowledge and correct use of renewable energies among primary and secondary school children, with the support of cartoons, multimedia films, artistic workshops, poems, etc. A further goal would be to spread the knowledge of good daily practices for an ecologically sustainable lifestyle.

Conclusions.

Reading projects from the European Commission on the development of a Green economy it emerges, that the main focus is always on the decarbonisation of the country (carbon neutrality, an area where multiple investments have been announced and committed by the Italian government), but nothing or little is available in terms of eco-adaptation, that is the response to challenges posed by climate change. Italy in particular is exposed to drought in the South of the country, floods and landslides in the alpine area, heat waves and impacts of rising sea, even more so than other European countries. Therefore, investments are needed to build new infrastructures, to create in each region adequate air conditioning in extreme heat and cold. Eco-adaptation can thus reduce the country's vulnerability to earthquakes, hydrogeological phenomena, and disastrous consequences for the environment, agriculture, etc. Moreover, drawing up a map of possible environmental eco-impacts is of great importance for the Green economy and a practical prerequisite for the formulation of a Green Law system, as described in this contribution. The Italian government needs to deliver concrete and targeted interventions in the matter of eco-adaptation, or the Green

New Deal will risk to become only a list of good intentions.

EJPLT

Un framework per il *contact tracing* in italia tra esigenze scientifiche, possibilità tecnologiche e rispetto di diritti e liberà individuali in termini di data protection

SERGIO GUIDA
Independent Researcher
Sr.Data/Information Governance Mgr.



Abstract

On March 11 the WHO declared COVID-19 a pandemic. Among quarantines and disruptions to public events, this also kick-started the expedited development of therapeutics and vaccines, but in the short time contact tracing, followed by treatment or isolation, is a key control measure.

A simple relationship was found between the efficiency necessary for eradication and the basic reproductive ratio of the disease, but being it a matter of controlling people and their movements, the extent and the ways in which controls can be implemented can also prove to be very invasive. So, various approaches and technological configurations have been developed as long as, depending on the use of geo-location and the methods and times of data storage, solutions that respect human rights and "privacy-preserving" have been identified, as indicated by the European Authorities, too.

Any solution should take care of its ethical implications, and be flexible enough to be improved rapidly, to rectify potential shortcomings and to avoid 'surveillance creep'. Last but not least, it must be designed to support full interoperability within the EU.

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Keywords: Pandemic - multipronged approach - spatial epidemiology - contact tracing - scope creep - cartography - public monitoring - geo-location - data protection by design - proportionality - electronic patient diary - privacy-preserving proximity tracing - function creep - surveillance creep.

Summary: Introduction – 1. Le prescrizioni del Garante Privacy e delle Autorità europee. 2. Razionale scientifico e richiami tecnici. – 3. Centralizzazione vs. decentralizzazione di dati e informazioni: differenze e conseguenze su data protection e privacy. – Conclusions.

Introduction.

Covid-19[1] è una malattia infettiva causata dal nuovo coronavirus SARS-COV-2[2], un beta coronavirus[3], che ha causato una pandemia globale con enormi perdite di vite umane: a livello globale, al 10 luglio 2020, ci sono stati 12.102.328 casi confermati, inclusi 551.046 decessi, segnalati all'OMS[4].

Attualmente, non esistono vaccini o trattamenti antivirali ufficialmente approvati per la prevenzione o la gestione della malattia[5], purtroppo.

Intanto, le misure necessarie per combatterlo hanno capovolto il nostro mondo, influenzando miliardi di persone e bloccando le economie.

Come ha detto Kristalina Georgieva, IMF *Managing Director*[6], questa è una crisi come nessun altra: "prevediamo la peggiore recessione economica dopo la Grande Depressione. Sebbene ci sia un'enorme incertezza sulla previsione, quest'anno prevediamo che la crescita globale scenderà del 3%. E prevediamo una ripresa parziale nel 2021, con una crescita prevista del 5,8 per cento"[7].

Ecco perché dopo la sospensione del Patto di stabilità "e la conseguente 'riscrittura' di alcune delle regole base della disciplina di bilancio europea (debito, deficit strutturale)" [8], "la

---

[1] Cfr. "Dal 2 gennaio 2020, i tre livelli dell'OMS (Ufficio nazionale cinese, Ufficio regionale per il Pacifico occidentale e quartier generale) collaborano per rispondere allo scoppio di COVID-19. Il 30 gennaio l'OMS ha dichiarato l'epidemia un'emergenza sanitaria pubblica di interesse internazionale (PHEIC). L'11 marzo, il Direttore Generale dell'OMS ha definito COVID-19 una pandemia" in https://www.who.int/westernpacific/emergencies/covid-19.

[2] Cfr. "L'11 febbraio 2020 il Comitato internazionale per la tassonomia dei virus (ICTV) ha annunciato la" sindrome respiratoria acuta grave coronavirus 2 (SARS-CoV-2) *severe acute respiratory syndrome–related coronavirus-2* "come nome del nuovo virus. Questo nome è stato scelto perché il virus è geneticamente correlato al coronavirus responsabile dell'epidemia di SARS del 2003. Sebbene correlati, i due virus sono diversi. (...) L'OMS ha annunciato "COVID-19" come nome di questa nuova malattia l'11 febbraio 2020" in https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it.

[3] Cfr. ad es. S. Dong, J. Sun, Z. Mao et Al., 'A guideline for homology modeling of the proteins from newly discovered betacoronavirus, 2019 novel coronavirus (2019-nCoV)', Journal of Medical Virology, 17 March 2020, https://doi.org/10.1002/jmv.25768.

[4] Fonte: WHO Coronavirus Disease (COVID-19) Dashboard , Data last updated: 2020/7/10, 3:54pm CEST.

[5] Cfr. N.L. Bragazzi, Y. Xiao, J. Wu et Al., 'An updated estimation of the risk of transmission of the novel coronavirus (2019-nCov)', Infectious Disease Modelling 5 (2020) 248-255, https://doi.org/10.1016/j.idm.2020.02.001, p. 249.

[6] Cfr. K. Georgieva, IMF Managing Director, 'Exceptional Times, Exceptional Action: Opening Remarks for Spring Meetings Press Conference', Washington, DC April 15, 2020 in https://www.imf.org/en/News/Articles/2020/04/15/ sp041520-exceptional-times-exceptional-action.

[7] Ibidem.

[8] Cfr. "Il 19 marzo 2020 la Commissione ha adottato un nuovo "Quadro Temporaneo" di aiuti di Stato a sostegno dell'economia nel contesto dell'epidemia di coronavirus, basato sull'articolo 107, paragrafo 3, lettera b), del Trattato sul funzionamento dell'Unione europea. Il quadro temporaneo riconosce che l'intera economia

pandemia che ha investito con la forza d'urto di uno tsunami l'economia europea e mondiale sta sostanzialmente ribaltando anche il rituale 'calendario' di finanza pubblica"[9].

"La conseguenza è che da noi il Governo, dall'esplodere del coronavirus, e al netto dei vari Dpcm che hanno scandito il *lockdown* dell'intero Paese, di fatto ha attuato misure urgenti sul piano economico che si configurano come una e più manovre economiche necessariamente anticipate rispetto alla rituale scadenza autunnale"[10].

Il Covid-19 ha travolto l'industria italiana[11]. La produzione industriale è crollata del 29,3%, una "caduta senza precedenti", anzi secondo ISTAT "in termini tendenziali l'indice corretto per gli effetti di calendario mostra una diminuzione che è la maggiore della serie storica disponibile (che parte dal 1990), superando i valori registrati nel corso della crisi del 2008-2009. Senza precedenti anche la caduta in termini mensili dell'indice destagionalizzato. Tutti i principali settori di attività economica registrano flessioni tendenziali e congiunturali, in molti casi di intensità inedite: nella fabbricazione di mezzi di trasporto e nelle industrie tessili, abbigliamento, pelli e accessori la caduta congiunturale e tendenziale supera ampiamente il 50%"[12].

In realtà, "l'area dell'euro sta affrontando una contrazione economica che per entità e rapidità non ha precedenti in tempi di pace. Le misure adottate per il contenimento della diffusione del coronavirus (COVID-19) hanno provocato un arresto di gran parte dell'attività economica in tutti paesi dell'area dell'euro e su scala mondiale"[13]

Di fronte alle gravissime emergenze da tutti i punti di vista, i governi di tutto il mondo si trovano a fronteggiare quello che molto argutamente è stato chiamato "il trilemma Covid-19"[14], schematizzato nella figura seguente:

dell'UE sta vivendo un grave turbamento. Consente agli Stati membri di utilizzare la piena flessibilità prevista dalle norme sugli aiuti di Stato per sostenere l'economia, limitando al contempo le conseguenze negative alla parità di condizioni nel Mercato Unico.".. "La Commissione europea ha adottato un primo emendamento il 3 aprile 2020 e un secondo oggi per estendere il campo di applicazione del Quadro Temporaneo sugli aiuti di Stato e consentire agli Stati membri di sostenere l'economia nel contesto dell'epidemia di coronavirus", recita la *Press Release* 8 May 2020 in https://ec.europa.eu/ commission/presscorner/detail/en/ip_20_838.

[9] Cfr. D. Pesole, 'Manovra da 80 miliardi tra marzo e maggio: come il Covid ha capovolto il calendario dei conti pubblici', 8 maggio 2020 in https://www.ilsole24ore.com/art/manovra-80-miliardi-marzo-e-maggio-come-covid-ha-capovolto-calendario-conti-pubblici-ADkePDP.

[10] Ibidem.

[11] Cfr. F. Gerosa, 'Il Covid-19 travolge l'industria italiana, tracollo record a marzo', Milano Finanza, 11/05/2020 in https://www.milanofinanza.it/news/il-covid-19-travolge-l-industria-italiana-tracollo-record-a-marzo-202005111052428 228.

[12] Cfr. Istat, 'Produzione industriale periodo di riferimento marzo 2020', Comunicato stampa 11/05/2020 in https://www.istat.it/it/files//2020/05/Produzione-industriale.pdf.

[13] Cfr. Banca d'Italia, 'Bollettino economico BCE, n. 3 – 2020' in https://www.bancaditalia.it/pubblicazioni/bollettino-eco-bce/2020/bol-eco-3-2020/index.html?com.dotmarketing.htmlpage.language=102&pk_campaign=EmailAlertBdi&_pk_kwd=it.

[14] Cfr. R. Bamford, H.Dace et al., 'A Price Worth Paying: Tech, Privacy and the Fight Against Covid-19', Institute for Global Change, 24 April 2020 in https://institute.global/policy/price-worth-paying-tech-privacy-and-fight-against-covid-19.

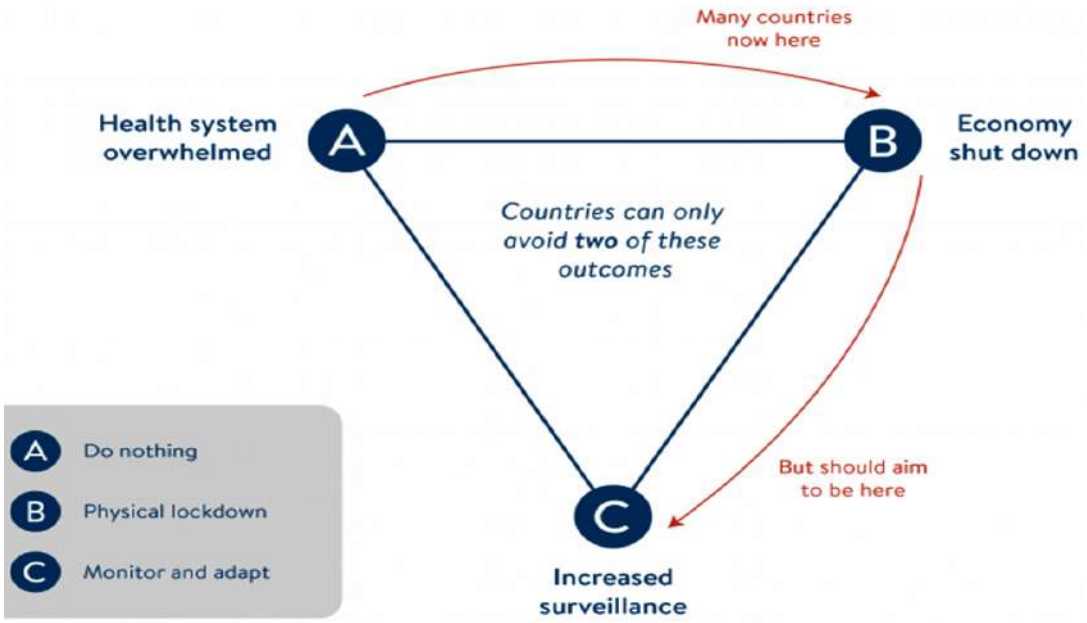


Figura 1: il "Trilemma Covid-19".

Una delle soluzioni più frequentemente proposte – ma, come vedremo con modalità che possono assumere varie connotazioni - è l'utilizzo di App di tracciamento dei contatti (*contact tracing*) per contenere e invertire la diffusione di COVID-19.

Molti sviluppatori "stanno lavorando su iniziative in parallelo e le autorità sanitarie pubbliche in un gran numero di paesi UE/SEE stanno esplorando diverse opzioni. È fondamentale che le autorità sanitarie pubbliche, gli epidemiologi e il personale coinvolti nelle operazioni quotidiane di tracciamento dei contatti siano strettamente coinvolti nel processo di sviluppo per garantire che le app funzionino secondo le migliori conoscenze disponibili sull'epidemiologia di COVID-19, e che le app mobili siano progettate per integrare gli sforzi di tracciamento dei contatti convenzionali"[15].

In effetti, il tracciamento dei contatti (*contact tracing*) è un mezzo[16] consolidato[17] per combattere la diffusione dell'infezione nelle popolazioni se integrata in una strategia di risposta alla salute più ampia e olistica[18]. Tradizionalmente un processo manuale per identificare con chi una persona infetta potrebbe essere entrata in contatto mentre era contagiosa è lungo e difficilmente scalabile per coprire popolazioni più grandi. Pertanto, per accelerare e dimensionare la risposta all'attuale pandemia di COVID-19, vengono progettate e sviluppate nuove soluzioni tecnologiche[19], che consentano di anticipare il momento in cui

[15] Cfr. European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020 in https://www.ecdc.europa.eu/en/publications-data/covid-19-mobile-applications-support-contact-tracing, pag.1.

[16] Cfr. M. Sampathkumar, 'What is contact tracing and can it help in the fight against coronavirus?' | Digital Trends, April 14, 2020 in https://www.digitaltrends.com/news/what-is-contact-tracing-and-how-can-it-help/.

[17] Ad es., "Contact tracing is one of the interventions that have been used to effectively control Ebola virus disease (EVD) outbreaks in Africa" in https://www.who.int/csr/disease/ebola/training/contact-tracing/en/.

[18] Cfr. B. Staehelin, C. Aptel, 'COVID-19 and contact tracing: a call for digital diligence', May 13, 2020 in https://media.ifrc.org/ifrc/2020/05/15/covid-19-contact-tracing-call-digital-diligence/.

[19] Cfr. Centers for Disease Control and Prevention (CDC), 'Contact Tracing : Part of a Multipronged Approach to Fight the COVID-19 Pandemic' in https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html.

la persona che *potrebbe* essere contagiosa può innanzitutto esserne messa a conoscenza, come nel seguente schema:

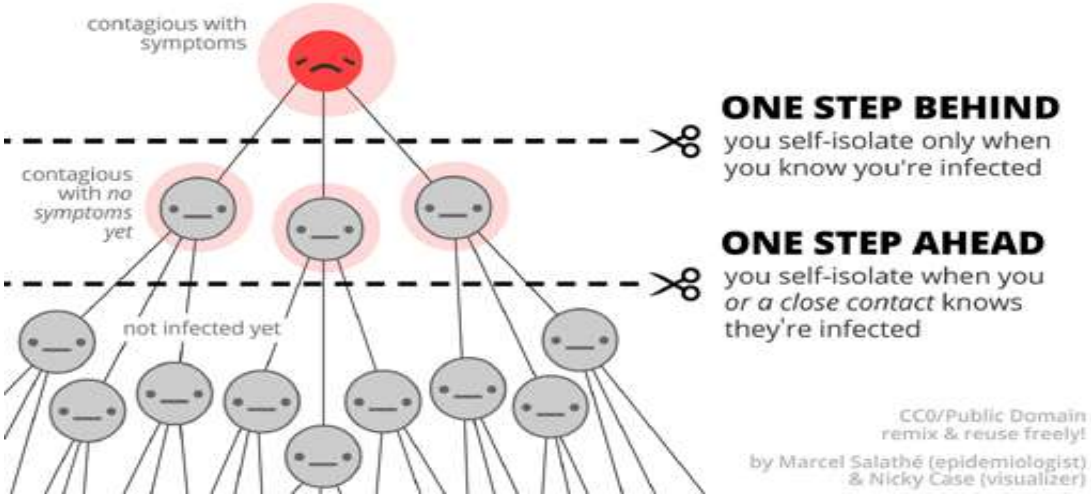


Figura 2: utilizzo del tracciamento dei contatti per limitare la diffusione di un virus.

La maggior parte delle implementazioni si concentra sulla notifica dell'esposizione: notificare a un utente che è stato vicino a un altro utente a cui è stata diagnosticata una diagnosi positiva e metterlo in contatto con le autorità sanitarie pubbliche. Questo tipo di App, che tendono a utilizzare il tracciamento della posizione o il monitoraggio della prossimità, può essere efficace nell'aiutare la lotta contro COVID-19 se esistono anche test diffusi e tracciabilità dei contatti basata su interviste.

In estrema sintesi, per il tracciamento dei contatti si rileva una *summa divisio* a seconda se avvenga:

A) utilizzando la geo-localizzazione: alcune App propongono di determinare quali coppie di persone sono state in contatto tra loro raccogliendo dati sulla posizione (compresi i dati GPS) per tutti gli utenti e cercando persone che si trovavano nello stesso posto contemporaneamente. Ma il rilevamento della posizione non è adatto alla ricerca dei contatti dei casi COVID-19, poiché i dati provenienti dal GPS di un telefono cellulare o dalle torri cellulari non sono semplicemente abbastanza precisi da indicare se due persone hanno avuto uno stretto contatto fisico (ovvero entro un raggio di circa 1,80 metri). Ma è abbastanza accurato per esporre informazioni sensibili e identificabili individualmente sulla casa, sul posto di lavoro e sulle abitudini di una persona.

B) utilizzando il 'monitoraggio di prossimità': le App di monitoraggio della prossimità utilizzano *Bluetooth Low Energy* (BLE)[20] per determinare se due *smartphone* sono abbastanza vicini da consentire ai loro utenti di trasmettere il virus. BLE misura la prossimità, non la posizione, e quindi è più adatto per la traccia dei contatti dei casi

[20] Cfr. "Ci sono due principali tecnologie nelle specifiche *Bluetooth: Bluetooth classic* e *Bluetooth Smart (Bluetooth Low Energy*). La principale differenza sta nel consumo di energia in ciascun caso. Tuttavia, ci sono altri fattori per cui *Bluetooth Smart* viene utilizzato per interessanti applicazioni tecnologiche."."2.Applicazioni - Il Bluetooth classico è ideale per le applicazioni che richiedono lo streaming continuo di dati, ad esempio le cuffie. Invece, *Bluetooth LE* è adatto per applicazioni che prevedono un trasferimento periodico di dati e ciò riduce una quantità significativa di utilizzo della batteria. Ciò rende BLE adatto per applicazioni IoT e di marketing di prossimità", M. Adarsh, 'Bluetooth Low Energy (BLE) beacon technology made simple: A complete guide to Bluetooth Low Energy Beacons', April 23, 2020 in https://blog.beaconstac.com/2018/08/ble-made-simple-a-complete-guide-to-ble-bluetooth-beacons/.

COVID-19 rispetto alle informazioni sulla posizione del cellulare o GPS. Quando due utenti dell'App si avvicinano, entrambi dispositivi stimano la loro vicinanza utilizzando la potenza del segnale Bluetooth. Se stimano che siano distanti meno di un metro e ottanta per un periodo di tempo sufficiente, ogni dispositivo registra un incontro con il codice dell'altro. Quando un utente dell'App viene a sapere di essere infetto da COVID-19, altri utenti possono essere informati del proprio rischio di infezione.

Tuttavia, l'uso di telefoni cellulari per le App di tracciamento dei contatti ha portato un intenso dibattito al crocevia di sanità pubblica, protezione dei dati e privacy. Anche la fiducia nella tecnologia e i potenziali interessi economici e strategici sono al centro della discussione. Fra le preoccupazioni principali: che la progettazione o l'utilizzo inadeguati di tali App possano portare a stigmatizzazione, aumento della vulnerabilità e fragilità, discriminazione, persecuzione e attacchi all'integrità fisica e psicologica di determinate popolazioni. Ciò tocca la questione più ampia dell'uso responsabile della tecnologia in contesti, come la risposta alle crisi, in cui la fiducia è fondamentale.

Il rischio poi che i dati raccolti allo scopo di tracciare i contatti possano essere utilizzati per altri scopi - o collegati ad altri set di dati per identificare e potenzialmente profilare ulteriori individui - è un aspetto centrale. Questo "*scope creep*" [21] potrebbe portare a sorveglianza intrusiva o uso commerciale non richiesto e indesiderato. Parallelamente, le App di tracciamento dei contatti non sono immuni da attacchi informatici e perdite di dati che potrebbero esporre la privacy e la sicurezza dei loro utenti.

Il tracciamento digitale dei contatti richiede inoltre controlli ed equilibri solidi ed efficaci per controllarne l'efficacia e garantire una gestione trasparente ed equa dell'ecosistema globale; la salute pubblica e i diritti individuali, specialmente in relazione alla privacy, devono poter lavorare di pari passo. Norme scientifiche, etiche e giuridiche aggiornate dovrebbero essere saldamente integrate in questo processo[22] e dovrebbero essere considerate valide solo le soluzioni basate su un approccio di 'protezione dei dati *by design*'.

Come vedremo, in questo contesto la '*data protection by design*' si basa su un'architettura decentralizzata progettata per mantenere il maggior numero possibile di dati particolari sui dispositivi degli utenti. Altre caratteristiche essenziali includono la limitazione dello scopo per mitigare il rischio di '*scope creep*' e un periodo di conservazione dei dati fissato, garantendo che gli strumenti digitali di tracciamento dei contatti vengano prontamente dismessi quando non sono più necessari.

Un esempio notevole di tale protocollo decentralizzato è quello proposto dal consorzio DP-3T [23], successivamente adottato ad es. dalla Croce Rossa austriaca [24] e dalla

[21] Nel *Project Management* con la locuzione '*Scope creep*' (cambiamento di ambito) ci si riferisce alla crescita continua o incontrollata nell'ambito di un progetto in qualsiasi momento dopo l'inizio del progetto stesso.

[22] Come si legge anche in European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020, cit., pag.1: "La prospettiva della salute pubblica dovrebbe essere al centro della valutazione dell'efficacia e della sicurezza delle app mobili. Inoltre, le app devono essere progettate in modo tale da consentire l'aggiornamento delle impostazioni e dei parametri. Pertanto, il focus di questa guida sono le considerazioni epidemiologiche e operative che le autorità sanitarie pubbliche potrebbero prendere in considerazione quando scelgono una soluzione o lavorano per implementare e valutare una particolare soluzione".

[23] Si veda ad es. in Github, DP-3T consortium e ampiamente *infra.*

[24] Cfr. 'Meet the STOPP CORONA APP' in https://www.roteskreuz.at/site/meet-the-stopp-corona-app/.

Confederazione Svizzera[25] e supportato dall'iniziativa Apple/Google[26].

1. Le prescrizioni del Garante Privacy e delle Autorità europee.

La nostra Autorità Garante è intervenuta in prima battuta il 2 febbraio 2020[27], quando "a seguito della Delibera del Consiglio dei Ministri del 31 gennaio 2020[28] con la quale è stato dichiarato, per sei mesi, lo stato di emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili, il Capo del Dipartimento della protezione civile ha chiesto con urgenza il parere del Garante in ordine a una bozza di ordinanza, contenente i primi interventi urgenti di protezione civile in relazione alla predetta emergenza, da emanarsi ai sensi dell´art. 25 del d.lgs. 2 gennaio 2018, n. 1, Codice della protezione civile"[29].

L'ordinanza, in relazione al trattamento dei dati personali connessi all'attuazione delle attività di protezione civile, allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, ha previsto che

- √ i soggetti operanti nel Servizio nazionale di protezione civile possono "effettuare trattamenti, compresa la comunicazione tra loro, di dati personali anche relativi agli artt. 9 e 10 del Regolamento (UE) 2016/679, che risultino necessari per l'espletamento della funzione di protezione civile fino al 30 giugno 2020"[30] .
- √ la comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli sopra citati, nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento (UE) 2016/679, è effettuata, nei casi in cui essa risulti indispensabile, ai fini dello svolgimento delle attività previste dall'ordinanza.
- √ i trattamenti di dati personali devono essere effettuati nel rispetto dei principi di cui all'art. 5 del Regolamento (UE) 2016/679"[31].

Il Garante "osserva che le disposizioni risultano idonee a rispettare le garanzie previste dalla normativa in materia di protezione dei dati personali nel contesto di una situazione di emergenza", evidenziando però come sia necessario "che, alla scadenza del termine dello stato di emergenza, siano adottate da parte di tutte le Amministrazioni coinvolte negli interventi di protezione civile misure idonee a ricondurre i trattamenti di dati personali

---

[25] Cfr. EPFL, 'Switzerland launches DP-3T contact tracing app', 21 April 2020 in https://privacyinternational.org/ examples/3726/switzerland-launches-dp-3t-contact-tracing-app.

[26] Cfr. Apple Newsroom, 'Apple and Google partner on COVID-19 contact tracing technology', April 10, 2020 in https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

[27] Cfr. Garante per la Protezione dei Dati Personali, Parere sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili – 2 febbraio 2020 [doc. web n. 9265883].

[28] Delibera del Consiglio dei Ministri 31 gennaio 2020, Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili. (20A00737) in GU n.26 del 1-2-2020.

[29] Con il Decreto Legislativo 2 gennaio 2018, n. 224, (Raccolta 2018) (18G00011), GU Serie Generale n.17 del 22-01-2018) è stato approvato il nuovo Codice della Protezione Civile, entrato in vigore il 6 febbraio 2018, e che ha abrogato, tra le altre, la legge 24 febbraio 1992, n. 225. Il Servizio nazionale della protezione civile è definito come il sistema che esercita la funzione di protezione civile costituita dall'insieme delle competenze e delle attività volte a tutelare la vita, l'integrità fisica, i beni, gli insediamenti, gli animali e l'ambiente dai danni o dal pericolo di danni derivanti da eventi calamitosi di origine naturale o derivanti dall'attività dell'uomo. Sono attività di protezione civile quelle volte alla previsione, prevenzione e mitigazione dei rischi, alla gestione delle emergenze e al loro superamento.

[30] Cfr. Garante per la Protezione dei Dati Personali, Parere sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili – 2 febbraio 2020 [doc. web n. 9265883], cit..

[31] Ibidem.

effettuati nel contesto dell'emergenza, all'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali in capo a tali soggetti".

Solo con queste premesse il Garante esprime "parere favorevole sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili"[32].

Il secondo intervento più significativo del Garante è stato quello con cui il 2 marzo ha stabilito che "Soggetti pubblici e privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti", dopo numerosi quesiti posti in merito alla possibilità di raccogliere, all'atto della registrazione di visitatori e utenti, informazioni circa la presenza di sintomi da Coronavirus e notizie sugli ultimi spostamenti, come misura di prevenzione dal contagio[33]. Analogamente, datori di lavoro pubblici e privati hanno chiesto al Garante la possibilità di acquisire una "autodichiarazione" da parte dei dipendenti in ordine all'assenza di sintomi influenzali, e vicende relative alla sfera privata.

Da un lato, la raccolta di informazioni relative ai sintomi e ai recenti spostamenti di ogni individuo spettano agli operatori sanitari e al sistema della protezione civile, vale a dire agli organi deputati a garantire il rispetto delle regole di sanità pubblica sancite.

Dall'altro, resta fermo l'obbligo del lavoratore di segnalare al datore di lavoro qualsiasi situazione di pericolo per la salute e la sicurezza sui luoghi di lavoro.

In tale quadro "il datore di lavoro può invitare i propri dipendenti a fare, ove necessario, tali comunicazioni agevolando le modalità di inoltro delle stesse, anche predisponendo canali dedicati; permangono altresì i compiti del datore di lavoro relativi alla necessità di comunicare agli organi preposti l'eventuale variazione del rischio 'biologico' derivante dal Coronavirus per la salute sul posto di lavoro e gli altri adempimenti connessi alla sorveglianza sanitaria sui lavoratori" attraverso l'opera del medico competente, come, ad esempio, la possibilità di sottoporre a una visita straordinaria i lavoratori più esposti.

Le autorità hanno, inoltre, previsto sia a livello nazionale che locale le misure di prevenzione necessarie per assicurare l'accesso dei visitatori a tutti i locali aperti al pubblico.

"Pertanto, il Garante invita tutti i titolari del trattamento ad attenersi scrupolosamente alle indicazioni fornite dal Ministero della salute e dalle istituzioni competenti per la prevenzione della diffusione del Coronavirus, senza effettuare iniziative autonome che prevedano la raccolta di dati anche sulla salute di utenti e lavoratori che non siano normativamente previste o disposte dagli organi competenti"[34].

Un altro intervento fondamentale è stata l'audizione informale del Presidente Soro sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus dinanzi alla Commissione Trasporti, Poste e Telecomunicazioni della Camera dei Deputati l'8 aprile 2020.

"La gravissima emergenza che il Paese sta affrontando ha imposto l'adozione- con norme di vario rango- di misure limitative di molti diritti fondamentali, necessarie per contenere auspicabilmente, il numero dei contagi"[35].

Alcune deroghe al regime ordinario di gestione dei dati sono state previste sin dalle

---

[32] Ibidem.

[33] Cfr. Garante per la Protezione dei Dati Personali, Coronavirus: Garante Privacy, no a iniziative "fai da te" nella raccolta dei dati. Soggetti pubblici e privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti – 2 marzo 2020 [doc. web n. 9282117].

[34] Ibidem.

[35] Cfr. A. Soro, Presidente del Garante per la protezione dei dati personali, 'Audizione informale, in videoconferenza, del sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus - Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati', 8 aprile 2020, riportato su sito Garante [doc. web n. 9308774].

primissime ordinanze intervenute pochi giorni dopo la deliberazione dello stato di emergenza, ma soprattutto "nuove e più invasive raccolte di dati potrebbero fondarsi su esigenze di sanità pubblica che -al pari del "soccorso di necessità"- costituiscono autonomi presupposti di liceità, in presenza di una previsione normativa conforme ai principi di necessità, proporzionalità, adeguatezza, nonché del rispetto del contenuto essenziale del diritto".

E' questa la cornice entro la quale valutare "l'ipotesi della raccolta dei dati sull'ubicazione o sull'interazione dei dispositivi mobili dei soggetti risultati positivi, con altri dispositivi, al fine di analizzare l'andamento epidemiologico o per ricostruire la catena dei contagi".

Dovendo privilegiare un criterio di gradualità, non pone particolari problemi l'acquisizione di trend, effettivamente anonimi, di mobilità. L'art. 9 della direttiva e-privacy legittima infatti il trattamento, anche in assenza del consenso dell'interessato, dei dati relativi all' ubicazione, purché anonimi.

Tale soluzione consente di realizzare, ad esempio, mappe descrittive dell'andamento dell'epidemia, utilissime a fini prognostici e statistici, meno a scopi diagnostici in senso proprio.

Per altro verso, l'uso di dati identificativi sull'ubicazione o sull'interazione con altri dispositivi può risultare funzionale a diversi scopi, , ma richiede – anche ai sensi dell'art. 15 della direttiva e-privacy – una disposizione normativa sufficientemente dettagliata e contenente adeguate garanzie.

I vari utilizzi possibili di tali dati possono essere finalizzati, in via teorica:

a) o alla verifica della posizione del soggetto sottoposto ad obbligo di permanenza domiciliare perché positivo, utilizzando dunque la geo-localizzazione del telefono (presupponendo segua continuamente il soggetto) per accertare l'effettivo rispetto del divieto di allontanamento dal domicilio, oppure:

b) all'acquisizione, a ritroso, dei dati sull'interazione del soggetto poi risultato positivo con altri soggetti, per verificarne, nel periodo in cui aveva capacità virale, gli eventuali contatti desumibili tramite varie tecniche: celle telefoniche, gps, *bluetooth*.

Le due ipotesi differiscono nella finalità, elemento decisivo per la valutazione della complessiva legittimità del trattamento.

La prima ipotesi infatti, nell'utilizzare la localizzazione del telefono come fosse una sorta di braccialetto elettronico atipico, presuppone la sostituzione, con l'occhio elettronico, dei controlli "umani", dando però per acquisito che chi decida di violare gli obblighi di permanenza domiciliare porti con sé il telefono, il che è evidentemente contro-intuitivo.

Più complessa è la seconda ipotesi, relativa alla mappatura a ritroso dei contatti tenuti, nel periodo d'incubazione, da soggetti risultati contagiati, cioè al *contact tracing*. Tale ricostruzione dei contatti può avvenire, almeno astrattamente, attraverso l'incrocio di tipologie di dati diversi: quelli sulle transazioni commerciali, sulle celle telefoniche, quelli sull'interazione con altri dispositivi mobili desunti dal ricorso a tecnologie *bluetooth*[36].

Va premesso che ciascuna tipologia di questi dati ha, naturalmente, una diversa significatività a fini epidemiologici, tanto maggiore quanto più idonea a selezionare i contatti più rilevanti perché più ravvicinati e, dunque, maggiormente suscettibili di aver determinato, almeno potenzialmente, un contagio, ma incide anche sul complessivo giudizio di proporzionalità, in quanto la maggiore selettività riduce il perimetro di incidenza della misura al solo stretto necessario, con effetti socialmente apprezzabili in termini di tutela della salute, individuale e collettiva.

[36] Per un'ampia disamina tecnica si veda ad es. K. Foy**, '**Bluetooth signals from your smartphone could automate Covid-19 contact tracing while preserving privacy', Lincoln Laboratory**,** MIT NEWS April 8, 2020 in https://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409.

In termini generali, comunque, il fine perseguito da tale misura risulta particolarmente apprezzabile perché non repressivo (come invece nel caso della sorveglianza del soggetto in quarantena obbligatoria mediante la sua geo-localizzazione), ma solidaristico.

Anche queste considerazioni inducono a preferire il ricorso a sistemi fondati sulla volontaria adesione dei singoli che consentano il tracciamento della propria posizione. Tuttavia, per garantire la reale libertà (e quindi la validità) del consenso al trattamento dei dati, esso non dovrebbe risultare in alcun modo condizionato[37].

Pertanto, non potrebbe ritenersi effettivamente valido, perché indebitamente e inevitabilmente condizionato, il consenso prestato al trattamento dei dati acquisiti con tali sistemi, se prefigurato come presupposto necessario, ad esempio, per usufruire di determinati servizi o beni (si pensi al sistema cinese).

L'efficacia diagnostica di tale soluzione dipende, in ogni caso, dal grado di adesione che essa incontri tra i cittadini, in quanto la rilevazione potrebbe per definizione avvenire solo limitatamente alla parte della popolazione che consenta di "farsi tracciare": la percentuale minima per l'efficacia è stimata nell'ordine del 60%.

In tal senso, quindi, la volontaria attivazione di un'App funzionale alla raccolta dei dati sull'interazione dei dispositivi, ben potrebbe rappresentare il presupposto di uno schema normativo fondato su esigenze di sanità pubblica, con adeguate garanzie per gli interessati (art. 9, p.2, lett. i) Reg. (Ue) 2016/679).

La seconda fase del trattamento (quella, cioè, successiva alla rilevazione dei dati) consiste essenzialmente nella conservazione degli stessi, in vista del loro eventuale, successivo utilizzo per allertare i potenziali contagiati.

Sotto il profilo dell'impatto sulla riservatezza, determinato dalla conservazione in sé dei dati, in vista del loro successivo utilizzo, è certamente preferibile la soluzione della registrazione del "diario dei contatti" sullo stesso dispositivo individuale nella disponibilità del soggetto. Si eviterebbe così la conservazione di dati personali in banche dati dei gestori, che riproporrebbe le criticità rilevate dalla giurisprudenza della Cgue sulla *data retention*[38].

I criteri di necessità, proporzionalità e minimizzazione rimarcati dalla giurisprudenza europea indicano, comunque, l'esigenza di contenere eventuali limitazioni della privacy nella misura strettamente necessaria a perseguire fini rilevanti, che garantisca cioè il minor ricorso possibile a dati identificativi, sia in fase di raccolta sia in fase di conservazione.

Ecco allora che il *bluetooth*, restituendo dati su interazioni più strette di quelle individuabili in celle telefoniche molto più ampie, si dimostra più efficace nel selezionare i possibili contagiati all'interno di un campione più attendibile proprio perché limitato ai contatti significativi.

In particolare, sarebbero apprezzabili quelle tecnologie che mantengono il diario dei contatti esclusivamente nella disponibilità dell'utente, sul suo dispositivo, ragionevolmente per il solo periodo massimo di potenziale incubazione. Il soggetto che risultasse positivo dovrebbe fornire l'identificativo Imei del proprio dispositivo all'ASL, che sarebbe poi tenuta a trasmetterlo al server centrale per consentirgli così di ricostruire, tramite un calcolo algoritmico, i contatti tenuti con altre persone le quali si siano, parimenti, avvalse dell'App *bluetooth*. Queste ultime riceverebbero poi un *alert* di potenziale contagio, con l'invito a

[37] Si veda, tra gli altri, L. Gatt, R. Montanari, I. A.Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali', Politica del diritto, 2017, 2, 337 – 353.

[38] Per tutte vedasi O. Pollicino, M. Bassini, 'La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico. Nota a Corte Giustizia UE, sent. 21 dicembre 2016, Tele2 e Watson, cause riunite C-203/15 e C-698/15', in Diritto Penale Contemporaneo https://archiviodpc.dirittopenaleuomo.org/upload/POLLICINOBASSINI_2017a.pdf.

sottoporsi ad accertamenti: in tal modo, il tracciamento sarebbe affidato a un flusso di dati pseudonimizzati, suscettibili di re-identificazione solo in caso di rilevata positività. La comunicazione tra server centrale ed App dei potenziali contagiati avverrebbe senza consentirne la re-identificazione, minimizzando l'impatto della misura sulla privacy individuale.

In alternativa all'*alert* intra-app, si potrebbe ipotizzare l'intervento diretto dell' ASL che informi e sottoponga ad accertamento le persone che, sulla scorta delle rilevazioni *bluetooth*, risultino avere avuto contatto con il soggetto positivo.

La conservazione dei dati di contatto, da parte del server, dovrebbe comunque limitarsi al tempo strettamente indispensabile alla rilevazione dei potenziali contagiati.

L'anamnesi rimessa al medico consentirebbe di evitare l'esclusiva soggezione a decisioni automatizzate, correggendo anche, così, possibili distorsioni e inesattezze nel processo algoritmico così come richiesto dal GDPR.

In ogni caso, è auspicabile che la complessa filiera del *contact tracing* possa realizzarsi interamente in ambito pubblico, fino a "prevedere specifici reati propri, suscettibili di realizzazione da parte di coloro che, potendo avere accesso ai dati per qualunque ragione anche operativa, li utilizzino per altre finalità".

"La soluzione ipotizzata ridurrebbe, verosimilmente allo stretto necessario, la sua incidenza sulla riservatezza. Tuttavia, benché non massivo, il trattamento di dati personali comunque realizzato richiederebbe, auspicabilmente, una norma di rango primario, quindi anche un decreto-legge, che assicura la tempestività dell'intervento, pur non omettendo il sindacato parlamentare né quello successivo di costituzionalità, diversamente dalle ordinanze"[39].

E sulla scorta di tale "auspicio" lo stesso Garante ha reso il Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 - 29 aprile 2020[40]: "la Presidenza del Consiglio dei Ministri ha richiesto il parere del Garante su una proposta normativa volta a disciplinare il trattamento di dati personali nel contesto dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del Covid-19 per finalità di tracciamento dei contatti tra i soggetti che, a tal fine, abbiano volontariamente installato un'apposita applicazione sui dispositivi mobili".

Al comma 1 si precisa che il titolare del trattamento è il Ministero della salute e che il trattamento riguarda il tracciamento effettuato tramite l'utilizzo di un'applicazione, installata su base volontaria e destinata alla registrazione dei soli contatti tra soggetti che abbiano parimenti scaricato l'applicazione. Ciò, al solo fine di adottare le adeguate misure di informazione e prevenzione sanitaria nel caso di soggetti entrati in contatto con utenti che risultino, all'esito di test o diagnosi medica, contagiati. Si prevede, in particolare, che il Ministero si coordini con i soggetti operanti nel Servizio nazionale della protezione civile, nonché con l'Istituto superiore di sanità, le strutture pubbliche e private accreditate che operano nell'ambito del Servizio sanitario nazionale, nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica da COVID-19. Si chiarisce, infine, che la modalità di tracciamento dei contatti tramite la piattaforma informatica di cui al predetto comma è complementare alle ordinarie modalità in uso nell'ambito del Servizio sanitario nazionale.

---

[39] Cfr. A. Soro, Presidente del Garante per la protezione dei dati personali, 'Audizione informale, in videoconferenza, del sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus - Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati', 8 aprile 2020 , riportato su sito Garante [doc. web n. 9308774], cit..

[40] Cfr. Garante per la Protezione dei Dati Personali, Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 - 29 aprile 2020 [doc. web n. 9328050].

Al comma 2 si prevede che, all'esito di una valutazione di impatto effettuata ai sensi dell'articolo 35 del Regolamento il Ministero della salute adotti misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati, sentito il Garante, assicurando, in particolare, che:

- gli utenti ricevano, prima dell'attivazione dell'App, un'idonea informativa;
- i dati personali raccolti dall'App siano esclusivamente quelli necessari ad avvisare gli utenti di rientrare tra i contatti stretti di altri utenti accertati positivi al Covid-19, individuati secondo criteri stabiliti dal Ministero della salute;
- il trattamento effettuato per il tracciamento sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati, con esclusione di ogni forma di geo-localizzazione dei singoli utenti;
- siano garantite su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché misure adeguate ad evitare il rischio di re-identificazione degli interessati cui si riferiscono i dati pseudonimizzati;
- i dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo, stabilito dal Ministero della salute, strettamente necessario al tracciamento e cancellati in modo automatico alla scadenza del termine; i diritti degli interessati di cui agli articoli da 15 a 22 del Regolamento possano essere esercitati anche con modalità semplificate.

Il comma 3 prevede che i dati raccolti attraverso l'App non possono essere utilizzati per finalità diverse da quella di cui al medesimo comma 1, salvo in forma aggregata o anonima per finalità scientifiche o statistiche.

Il successivo comma 4 stabilisce che il mancato utilizzo dell'App non comporta conseguenze in ordine all'esercizio dei diritti fondamentali dei soggetti interessati ed è assicurato il rispetto del principio di parità di trattamento, mentre il comma 5 prevede che la piattaforma informatica utilizzata è realizzata esclusivamente con infrastrutture localizzate sul territorio nazionale e gestite da amministrazioni o enti pubblici o in controllo pubblico.

Infine il comma 6 chiarisce che ogni trattamento di dati personali dovrà cessare al termine del periodo di emergenza secondo la tempistica espressamente indicata, con conseguente cancellazione dei dati trattati.

Viene subito rilevato che "la norma tiene conto di molte delle indicazioni fornite dal Presidente del Garante nell'audizione tenuta in data 8 aprile u. presso la IX Commissione trasporti e comunicazioni della Camera dei deputati"(*ut supra*), così come "appare conforme, per quanto dalla stessa disciplinato e nelle sue linee generali, ai criteri indicati dalle Linee guida del Comitato europeo per la protezione dei dati del 21 aprile scorso (vedi *infra*) a proposito dei sistemi di *contact tracing*, che possono sintetizzarsi nei termini seguenti, raffrontandovi la disposizione in esame:

a) volontarietà: in ragione del rilevante impatto individuale del tracciamento, l'adesione deve essere frutto di una scelta realmente libera da parte dell'interessato. La mancata adesione al sistema non deve quindi comportare conseguenze pregiudizievoli, adottando dunque una locuzione più ampia di quella riferita al solo esercizio dei diritti fondamentali;

b) previsione normativa: il presupposto può individuarsi nell'esigenza di svolgimento di un compito di interesse pubblico, in particolare per esigenze di sanità pubblica, in base a "previsione normativa o disposizione legislativa" dell'Unione europea o degli Stati membri. Sotto questo profilo, in particolare, la scelta di una norma di rango primario soddisfa i

requisiti di cui all'articolo 9, par. 2, lett. i) del Regolamento[41] e agli articoli 2-ter e 2-sexies del Codice[42], con garanzie ulteriori che potranno essere stabilite con il previsto provvedimento del Garante da adottare ai sensi dell'articolo 2-quinquiesdecies del medesimo Codice;

c) trasparenza: in linea con tale esigenza è la previsione di cui all'articolo 1, comma 2, lett. a), della norma che assicura agli interessati un'idonea informazione sul trattamento e in particolare sulla pseudonimizzazione dei dati, mentre si raccomanda all'Amministrazione interessata di sottoporre la valutazione di impatto cui è tenuta al più ampio regime di conoscibilità e di prevedere, anche nella norma, il carattere libero e aperto del software da rilasciare con licenza open source;

d) determinatezza ed esclusività dello scopo: il *tracing* dev'essere finalizzato esclusivamente al contenimento dei contagi, escludendo fini ulteriori, ferme restando le possibilità di utilizzo a fini di ricerca scientifica e statistica, purché nei soli termini generali previsti dal Regolamento;.

e) selettività e minimizzazione dei dati: i dati raccolti devono poter tracciare i contatti stretti e non i movimenti o l'ubicazione del soggetto. Devono essere raccolti solo i dati strettamente necessari ai fini della individuazione dei possibili contagi, con tecniche di anonimizzazione e pseudonimizzazione affidabili. Anche la conservazione deve limitarsi al periodo strettamente necessario, da valutarsi sulla base delle decisioni dell'autorità sanitaria su parametri oggettivi come il periodo di incubazione. A tal riguardo le disposizioni dello schema di norma su tali aspetti è opportuno che siano ulteriormente articolate in sede di attuazione dal Ministero della salute ai sensi del comma 2, anche con riferimento alla sorte dei dati raccolti sul dispositivo di chi, in un momento successivo all'installazione dell'applicazione, abbia poi deciso di disinstallarla;

f) non esclusività del processo algoritmico e possibilità di esercitare in ogni momento i diritti di cui agli articoli da 15 a 22 del Regolamento;

g) interoperabilità con altri sistemi di *contact tracing* utilizzati in Europa. Tali caratteristiche di interoperabilità potranno essere assicurate in sede applicativa e, ancor prima, nell'ambito dei provvedimenti di competenza del Ministero;

h) reciprocità di anonimato tra gli utenti dell'App, i quali devono peraltro non essere identificabili dal titolare del trattamento, dovendo la identificazione ammettersi al limitato fine dell'individuazione dei contagiati. La norma, alla lettera e), non specifica chiaramente se si intenda optare per la conservazione dei dati in forma centralizzata ovvero decentrata. In ogni caso, la centralizzazione richiederebbe in sede attuativa la previsione di misure di sicurezza rafforzate, adeguate alla fattispecie.

In sintesi, dunque, un sistema di *contact tracing* come descritto non sarebbe in contrasto con i principi di protezione dei dati personali. Anzi, come passiamo a vedere, sono gli stessi criteri enunciati e dettagliati più volte dalle Autorità europee**.**

Già nel suo primo intervento in materia, il Comitato europeo per la protezione dei dati (EDPB, *European Data Protection Board*) ha infatti ricordato[43] che gli sforzi per utilizzare i dati di geo-localizzazione per effettuare il tracciamento dei contatti - in effetti nello stesso modo

---

[41] Regolamento generale sulla protezione dei dati (GDPR): Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale UE 127 del 23/05/2018.

[42] Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (in S.O. n.123 alla G.U. 29/07/2003, n.174) integrato con le modifiche introdotte dal D.Lgs.10 agosto2018, n.101 (in G.U. 04/09/2018 n.205).

[43] Cfr. European Data Protection Board, Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak, 16 March, 2020 in https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en.

in cui alcuni paesi prevedono controverse - sarebbero attualmente illegali ai sensi della direttiva e-privacy[44]. Ma in determinate circostanze, comprese le questioni di sicurezza nazionale e pubblica, gli Stati membri hanno il titolo di introdurre nuove leggi che sostituiranno le loro interpretazioni esistenti della direttiva.

Nella dichiarazione leggiamo: "Le leggi nazionali di attuazione della direttiva e-privacy prevedono il principio secondo cui i dati di localizzazione possono essere utilizzati dall'operatore solo quando sono resi anonimi o con il consenso delle persone".

"Le autorità pubbliche dovrebbero in primo luogo mirare al trattamento dei dati relativi all'ubicazione in modo anonimo (ovvero l'elaborazione dei dati aggregati in modo tale da non poter essere convertiti in dati personali). Ciò potrebbe consentire di generare rapporti sulla concentrazione di dispositivi mobili in una determinata posizione ('cartografia')".

In pratica, per identificare gruppi di persone che infrangevano le regole di autoisolamento le forze dell'ordine potevano usare dati aggregati sulla posizione, basati sulla vicinanza delle persone alle torri cellulari, ma non potevano usare i dati per trovare persone che erano venute a stretto contatto con quelli che in seguito erano risultati positivi.

La dichiarazione continua: "Quando non è possibile elaborare solo dati anonimi, l'art. 15 della direttiva e-privacy[45] consente agli Stati membri di introdurre misure legislative per la sicurezza nazionale e pubblica.

"Questa legislazione di emergenza è possibile a condizione che costituisca una misura necessaria, appropriata e proporzionata all'interno di una società democratica. Se vengono introdotte misure di questo tipo, uno Stato membro è tenuto a istituire garanzie adeguate, come garantire ai singoli il diritto a un ricorso giurisdizionale."

Riguardo al GDPR[46],"prevede le basi legali per consentire ai datori di lavoro e alle autorità sanitarie competenti di trattare i dati personali nel contesto di epidemie, senza la necessità di ottenere il consenso dell'interessato".

---

[44] Direttiva 2002/58 / CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla protezione della vita privata nel settore delle comunicazioni elettroniche (Direttiva sulla privacy e le comunicazioni elettroniche). "Conosciuta come Direttiva e-Privacy, stabilisce le regole su come i fornitori di servizi di comunicazione elettronica, come le società di telecomunicazioni e i fornitori di servizi Internet, dovrebbero gestire i dati dei loro abbonati. Garantisce inoltre i diritti per gli abbonati quando utilizzano questi servizi ". (...) "Nel giugno 2013 la Commissione ha messo in atto nuove norme specifiche per garantire che le violazioni dei dati personali nel settore delle telecomunicazioni dell'UE siano notificate allo stesso modo in ciascuno Stato membro." In https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive.

[45] Il testo consolidato recita "Articolo 15 Applicazione di alcune disposizioni della direttiva 95/46 / CE - 1. Gli Stati membri possono adottare misure legislative per limitare la portata dei diritti e degli obblighi di cui all'articolo 5, all'articolo 6, all'articolo 8, paragrafo 1 , (2), (3) e (4) e dell'articolo 9 della presente direttiva quando tale restrizione costituisce una misura necessaria, appropriata e proporzionata all'interno di una società democratica per salvaguardare la sicurezza nazionale (vale a dire la sicurezza dello Stato), la difesa, la pubblica sicurezza e la prevenzione, l'indagine, l'individuazione e il perseguimento di reati o dell'uso non autorizzato del sistema di comunicazione elettronica, di cui all'articolo 13, paragrafo 1, della direttiva 95/46 / CE. A tal fine, gli Stati membri possono, tra l'altro, adottare misure legislative che prevedono la conservazione di dati per un periodo limitato giustificato dai motivi di cui al presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea. " - "1b. I fornitori istituiscono procedure interne per rispondere alle richieste di accesso ai dati personali degli utenti sulla base delle disposizioni nazionali adottate ai sensi del paragrafo 1. Forniscono all'autorità nazionale competente, su richiesta, informazioni su tali procedure, il numero di richieste ricevute, il giustificazione legale invocata e loro risposta" in https://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058 :20091219:EN:HTML.

[46] Come noto, "il Regolamento generale sulla protezione dei dati (GDPR) dell'UE garantisce che i dati personali possano essere raccolti solo a condizioni rigorose e per scopi legittimi. Le organizzazioni che raccolgono e gestiscono le tue informazioni personali devono anche proteggerle dall'uso improprio e rispettare determinati diritti" in https://ec.europa.eu/digital-single-market/en/online-privacy.

Andrea Jelinek, presidente di EDPB, afferma: "Le norme sulla protezione dei dati (come il GDPR) non ostacolano le misure prese nella lotta contro la pandemia di coronavirus. Tuttavia, vorrei sottolineare che, anche in questi tempi eccezionali, il responsabile del trattamento dei dati deve garantire la protezione dei dati personali degli interessati. Pertanto, una serie di considerazioni dovrebbero essere prese in considerazione per garantire il trattamento legale dei dati personali. "

Quindi, lo scopo principale della dichiarazione EDPB è ricordare che le protezioni del GDPR non possono semplicemente essere spazzate via anche durante una crisi di salute pubblica[47].

In effetti, a partire dal fatto che l'enorme capacità di elaborazione dei dati consentita dalla tecnologia ha un impatto significativo sulla vita di ogni singolo cittadino e in linea con il *Necessity Toolkit*[48] del 2017, che aveva delimitato la portata del concetto di necessità di limitazioni ai diritti fondamentali, il GEPD ha adottato a dicembre 2019 i nuovi «orientamenti sulla proporzionalità»[49].

Tali regole definiscono ulteriormente il contenuto e lo scopo dei diritti garantiti dalla Carta fondamentale e dal GDPR, sviluppando un'analisi giuridica approfondita volta a creare un vero test di proporzionalità e strumenti pratici per aiutare a valutare la conformità delle misure UE proposte che avrebbero un impatto sui fondamentali diritti alla privacy e protezione dei dati personali[50].

Un ultimo punto: la fase di "proporzionalità in senso stretto" esamina gli effetti dell'atto legislativo, confrontando e ponderando i benefici derivanti dal perseguimento dell'obiettivo a cui mira il legislatore e i costi, cioè i sacrifici che esso impone agli altri diritti e interessi in gioco[51].

Normalmente è la valutazione più delicata, "quella che richiede al giudice di allargare lo sguardo delle sue valutazioni, fino a proiettarsi sull'impatto effettivo della legislazione che gli viene presentata: ciò richiede una conoscenza dei dati dell'esperienza reale che la legge regola, che supera di gran lunga i dati legali positivi, strettamente inteso"[52].

In pratica il rischio che la necessaria serenità di giudizio possa essere influenzata dall'urgenza di utilizzare al più presto strumenti tecnologici pervasivi ma efficaci per limitare pandemie così contagiose come Covid-19 deve essere attentamente valutato.

---

[47] Cfr. "Sono rigorose regole di protezione dei dati per garantire il diritto fondamentale alla protezione dei dati personali. Sono fondamentali per una società democratica e una componente importante di un'economia sempre più basata sui dati. L'UE aspira a cogliere le numerose opportunità offerte dalla trasformazione digitale in termini di servizi, posti di lavoro e innovazione, affrontando al contempo le sfide che queste comportano." nella Comunicazione della Commissione al Parlamento europeo e al Consiglio, Norme sulla protezione dei dati come strumento per rafforzare la fiducia nell'UE e oltre, Bruxelles, 24.7.2019, pagina 1, https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/communication_2019374_final.pdf.

[48] Cfr. Garante Europeo per la Protezione dei Dati, 'Valutare la necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali: A Toolkit', 11 aprile 2017 in https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

[49] Cfr. Garante Europeo per la Protezione dei Dati, Linee guida sulla valutazione della proporzionalità delle misure che limitano i diritti fondamentali alla privacy e alla protezione dei dati personali, 19 dicembre 2019 in https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en.

[50] Vedi anche S. Guida, D. Tozzi, 'La valutazione della proporzionalità delle misure che limitano i diritti fondamentali della privacy nelle nuove linee guida del garante europeo della protezione dei dati' in European Journal of Privacy Law & Technologies, ISSN 2704-8012, Issue 2020/1 – 2020.

[51] Cfr. M. Cartabia, 'I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana, Conferenza trilaterale delle Corte costituzionali italiana, portoghese e spagnola', Roma, Palazzo della Consulta 24-26 ottobre 2013, Working Papers, pag.5.

[52] Ibidem.

Sostanzialmente, EDPB sembra voler riaffermare il suo orientamento secondo cui "le decisioni di progettazione tecnologica non dovrebbero dettare le nostre interazioni sociali e la struttura delle nostre comunità, ma dovrebbero piuttosto sostenere i nostri valori e diritti fondamentali"[53].

Tuttavia, non si deve mai dimenticare che "lo spettro di osservazione dell'esperienza legale (...) è particolarmente ampio e, quindi, adeguato al giudizio di ragionevolezza"[54].

E infine "Ragionevole non esprime solo pura razionalità, ma, come è stato effettivamente detto con parole pertinenti anche all'universo legale, consiste nel sottomettere la ragione all'esperienza"[55].

Tanto che pochi giorni dopo il Comitato Europeo per la Protezione dei Dati ha adottato la "Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19"[56], che per sviluppare quanto già espresso dalla Presidente, Andrea Jelinek, *ut supra*.

Il 30/03/2020 il Consiglio d'Europa (*CoE*) ha pubblicato il documento intitolato "Dichiarazione comune sul diritto alla protezione dei dati nel contesto della pandemia di COVID-19 di Alessandra Pierucci, presidente del Comitato delle convenzioni 108 e Jean Philippe Walter, Commissario per la protezione dei dati del Consiglio d'Europa"[57]. Il documento si articola in 5 punti: elaborazione di dati relativi alla salute; 2. Elaborazione dei dati su larga scala; 3. Trattamento dei dati da parte dei datori di lavoro; 4. Dati da Mobile, e da computer; 5. Elaborazione dei dati nei sistemi educativi.

Lo snodo centrale di questo documento è il seguente: secondo la Convenzione 108+ (art.11) per possibili restrizioni in tempi di pandemia le eccezioni devono essere "previste dalla legge, rispettare l'essenza dei diritti e delle libertà fondamentali e costituisce una misura necessaria e proporzionata in una società democratica".

L'8/04/2020 la Commissione europea ha pubblicato la "Raccomandazione su un approccio comune dell'Unione per l'uso della tecnologia e dei dati per combattere e uscire dalla crisi COVID-19, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati di mobilità anonimizzati"[58].

Gli obiettivi della raccomandazione sono così indicati: "questa raccomandazione istituisce un processo per lo sviluppo di un approccio comune, denominato *Toolbox*, per utilizzare i mezzi digitali per affrontare la crisi. La cassetta degli attrezzi consisterà in misure pratiche per un uso efficace di tecnologie e dati, con particolare attenzione a due aree in particolare:

(1) ***Un approccio paneuropeo per l'uso di applicazioni mobili****, coordinato a livello dell'Unione, per consentire ai cittadini di adottare misure di distanziamento sociale efficaci e più mirate e per*

---

[53] Cfr. Garante Europeo per la Protezione dei Dati, Parere 4/2015 Verso una nuova etica digitale Dati, dignità e tecnologia 11 settembre 2015, pag. 10 in https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_it.pdf.

[54] Cfr. M. Cartabia, 'I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana, Conferenza trilaterale delle Corte costituzionali italiana, portoghese e spagnola', Roma, Palazzo della Consulta 24-26 ottobre 2013, Working Papers, cit., pag.19.

[55] Ibidem.

[56] European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020 in https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en.

[57] Cfr. Council of Europe, Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 30 March 2020 in https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter.

[58] Cfr. European Commission, Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data in https://ec.europa.eu/info/sites/info/files/recommendation_on apps_for_contact_tracing_4.pdf.

avvertire, prevenire e tracciare i contatti per contribuire a limitare la propagazione della malattia COVID-19. Ciò comporterà una metodologia per il monitoraggio e la condivisione delle valutazioni dell'efficacia di tali applicazioni, della loro interoperabilità[59] *e delle implicazioni transnazionali e del loro rispetto per la sicurezza, la privacy e la protezione dei dati; e*

(2) ***Uno schema comune per l'utilizzo di dati anonimi e aggregati sulla mobilità delle popolazioni*** *al fine di (i) modellare e prevedere l'evoluzione della malattia, (ii) monitorare l'efficacia del processo decisionale da parte delle autorità degli Stati membri su misure come il distanziamento sociale e confinamento e (iii) informare una strategia coordinata per uscire dalla crisi COVID-19".*

Nella stessa data, il Comitato dei Ministri del Consiglio d'Europa ha pubblicato la "Raccomandazione CM / Rec (2020) 1 del Comitato dei Ministri agli Stati membri sugli impatti dei diritti umani dei sistemi algoritmici (adottata dal Comitato dei Ministri su 8 aprile 2020 alla 1373a riunione dei deputati dei ministri)"[60]. Questa raccomandazione, breve ma con un allegato molto ampio (Linee guida), evidenzia ovviamente gli aspetti relativi ai diritti umani.

Il 21 aprile 2020, durante la sua 23a sessione plenaria, l'EDPB ha adottato linee guida sul trattamento dei dati sanitari a fini di ricerca nel contesto dell'epidemia COVID-19 e linee guida sulla geo-localizzazione e altri strumenti di tracciabilità nel contesto dell'epidemia COVID-19. Entrambe eccezionalmente non saranno sottoposte a consultazione pubblica a causa dell'urgenza della situazione attuale e della necessità di avere le linee guida prontamente disponibili.

Le "linee guida sul trattamento dei dati sanitari a fini di ricerca nel contesto dell'epidemia COVID-19"[61] mirano a far luce sulle questioni legali più urgenti relative all'uso dei dati sanitari, come la base giuridica del trattamento, l'ulteriore trattamento dei dati sanitari ai fini della ricerca scientifica, l'implementazione di garanzie adeguate e l'esercizio dei diritti dell'interessato.

Le linee guida affermano che il GDPR contiene diverse disposizioni per il trattamento dei

---

[59] In tema di "interoperabilità transfrontaliera, ci sono alcuni aspetti epidemiologici da considerare. App diverse hanno algoritmi di calcolo del rischio diversi sebbene tutti saranno basati sul tempo e sulla distanza come parametri di base. Alcuni possono utilizzare un cut-off tale che deve essersi verificata un'esposizione a meno di due metri per più di 15 minuti mentre altri possono tenere conto di diverse combinazioni di tempo e distanza, esposizione cumulativa e altri parametri come l'insorgenza dei sintomi a calcolare un punteggio di rischio. Si consiglia di scambiare informazioni tra le app in modo da consentire l'esecuzione di diversi tipi di calcoli del rischio. Tali informazioni includerebbero il tempo e la distanza delle esposizioni, comprese quelle di breve durata come cinque minuti (o meno, se del caso). Vi sono alcune considerazioni operative aggiuntive relative al viaggio. Scenario di esempio: un cittadino e un utente dell'app dal Paese A (utente A) si recano nel Paese B per un periodo di tempo. Quando si trova nel paese B, entra in contatto con un cittadino del paese B (utente B) che in seguito risulta positivo. L'utente A riceverà una notifica. Se l'utente A si trova ancora nel paese B in quel momento, le autorità sanitarie pubbliche devono considerare da quale paese / i dovrebbe ricevere la notifica. Il modo più semplice sarebbe quello di ricevere la notifica attraverso la propria app dal Paese A. Le informazioni saranno nella lingua (e) che capisce e da un'autorità fidata. Tuttavia, potrebbe non disporre di informazioni localmente appropriate. Le autorità sanitarie pubbliche potrebbero anche prendere in considerazione la possibilità di collaborare con gli sviluppatori di app per consentire di adattare i consigli di conseguenza, ad esempio fornendo un numero di follow-up da chiamare rilevante per il Paese di visita" in European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020, cit., pag.8.

[60] Council of Europe, Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies in https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

[61] Cfr. European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21 April 2020 in https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en.

dati sanitari ai fini della ricerca scientifica, che si applicano anche nel contesto della pandemia di COVID-19, in particolare per quanto riguarda il consenso e le rispettive legislazioni nazionali. Il GDPR prevede la possibilità di elaborare determinate categorie speciali di dati personali, come i dati sanitari, laddove sia necessario per scopi di ricerca scientifica.

Inoltre, le linee guida affrontano questioni legali relative ai trasferimenti internazionali di dati che coinvolgono dati sanitari a fini di ricerca relativi alla lotta contro COVID-19, in particolare in assenza di una decisione di adeguatezza o di altre garanzie appropriate.

Le "linee guida sulla geo-localizzazione e altri strumenti di tracciamento nel contesto dell'epidemia COVID-19" [62] mirano a chiarire le condizioni e i principi per l'uso proporzionato dei dati di localizzazione e degli strumenti di tracciamento dei contatti, per due scopi specifici:

1. utilizzare i dati di localizzazione per supportare la risposta alla pandemia modellando la diffusione del virus al fine di valutare l'efficacia complessiva delle misure di confinamento;

2. utilizzare il tracciamento dei contatti, che ha lo scopo di informare le persone che potrebbero essere state vicine a qualcuno che alla fine è stato confermato come portatore del virus, al fine di rompere le catene di contaminazione il prima possibile.

Le linee guida sottolineano che sia il GDPR che la Direttiva *ePrivacy* contengono disposizioni specifiche che consentono l'uso di dati anonimi o personali per supportare le autorità pubbliche e altri attori sia a livello nazionale che dell'UE nei loro sforzi per monitorare e contenere la diffusione di COVID-19. I principi generali di efficacia, necessità e proporzionalità devono guidare qualsiasi misura adottata dagli Stati membri o dalle istituzioni dell'UE che comporta il trattamento di dati personali per combattere COVID-19.

L'EDPB sostiene e sottolinea la posizione espressa nella sua lettera alla Commissione europea del 14 aprile[63] secondo cui l'uso delle app di tracciamento dei contatti dovrebbe essere volontario e non dovrebbe fare affidamento sulla traccia dei singoli movimenti, ma piuttosto sulle informazioni di prossimità riguardanti gli utenti.

La dott.ssa Jelinek ha aggiunto: "Le app non possono mai sostituire infermieri e medici. Sebbene i dati e la tecnologia possano essere strumenti importanti, dobbiamo tenere presente che hanno limiti intrinseci. Le App possono solo integrare l'efficacia delle misure di sanità pubblica e la dedizione degli operatori sanitari necessaria per combattere COVID-19. Ad ogni modo, le persone non dovrebbero essere messe di fronte a dover scegliere tra una risposta efficace alla crisi e la protezione dei diritti fondamentali".

In data 7 maggio 2020 l'Unità Tecnologie e Privacy del Garante europeo ha emanato il "documento tecnico 1/2020 sul tracciamento dei contatti con Applicazioni Mobili"[64]. Esso "ha lo scopo di fornire una descrizione fattuale di una tecnologia emergente e discutere i suoi possibili impatti sulla privacy e sulla protezione dei dati personali. I contenuti di questa pubblicazione non implicano una posizione politica del GEPD". In realtà, contiene una serie di dettagli tecnici molto importanti, ad.es.:

√ *Tracciamento di prossimità digitale*

Per supportare e integrare il tracciamento tradizionale, potrebbero essere utilizzati i

---

[62] Cfr. European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020 in https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_en.

[63] Cfr. European Data Protection Board, Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, 14 April 2020 in https://edpb.europa.eu/news/news/2020/twenty-first-plenary-session-european-data-protection-board-letter-concerning_it.

[64] European Data Protection Supervisor, TechDispatch #1/2020: Contact Tracing with Mobile Applications, 7 May 2020, in https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en.

sensori di onde radio integrati: lo *smartphone* potrebbe essere utilizzato, con l'installazione di un'applicazione dedicata e/o l'aggiornamento del software del sistema operativo[65], per registrare quando due persone sono abbastanza vicine per un tempo sufficientemente lungo affinché esista un rischio elevato di contagio.

√ *Quali sono le implicazioni sulla protezione dei dati?*

Il tracciamento dei contatti di prossimità sia tradizionale che digitale comporta il trattamento di dati personali. Laddove i dati si riferiscono a persone infette, si tratta di dati sanitari che richiedono una protezione speciale.

√ *Sorveglianza su larga scala*

Il tracciamento di prossimità digitale comporta nuovi rischi per la protezione dei dati in quanto prevede la registrazione preventiva e per contatto di un numero molto elevato di popolazione negli spazi pubblici e privati utilizzando segnali di onde radio.

È quindi probabile che le applicazioni di tracciamento dei contatti comportino un rischio elevato per i diritti e le libertà delle persone fisiche e richiedano una valutazione dell'impatto sulla protezione dei dati da condurre prima del loro spiegamento.

√ *Identificazione dell'utente*

I contatti di un caso possono includere familiari, vicini o colleghi di lavoro. Collegato ad altri dati, ad es. dai social network, è tecnicamente possibile risalire al nome della persona infetta, il luogo di residenza e di lavoro e una serie di altre attività e potenzialmente la sua posizione. Il numero di contatti e la loro frequenza possono persino rivelare abitudini sociali, come le pratiche religiose. Il collegamento con i dati sulla posizione, come accade con la traccia basata sul GPS, potrebbe consentire di dedurre un'immagine dettagliata della routine quotidiana.

Le tecnologie di minimizzazione dei dati e di miglioramento della privacy possono quindi prevenire danni attraverso l'identificazione di contatti e casi infetti.

Poiché le App di tracciamento possono funzionare senza l'identificazione diretta dei loro utenti, è necessario adottare misure appropriate per prevenire la re-identificazione. Ad es., poiché i dati sulla posizione sono inclini alla re-identificazione, è meglio evitare la traccia basata sulla posizione. Le applicazioni per *smartphone* di tracciamento di prossimità digitale non richiedono il monitoraggio della posizione dei singoli utenti. Invece, dovrebbero essere utilizzati i dati di prossimità, in particolare ottenuti tramite Bluetooth BLE (*ut supra*).

Le App di tracciamento possono utilizzare identificatori pseudonimizzati per i contatti di prossimità e modificarli periodicamente, ad esempio ogni 30 minuti. Ciò riduce il rischio di collegamento e re-identificazione dei dati. Gli schemi di condivisione segreti consentono di dividere gli identificatori in parti e di diffondere la loro trasmissione in un determinato periodo di tempo. Eventuali attaccanti che tentassero di rivelare e mappare i contatti dovrebbero attendere per ricevere il numero minimo di parti necessarie per riassemblare nuovamente l'identificatore.

Il servizio che fornisce test e conferma dello stato di infezione può operare indipendentemente dal servizio centrale al quale i casi caricano i dati di tracciamento dei contatti per impedire il collegamento dei dati di tracciamento ai file dei casi medici. Per garantire comunque che i dati vengano caricati solo da casi confermati, il servizio centrale potrebbe richiedere una prova digitale.

√ *Limitazioni delle finalità*

E' necessario determinare in anticipo per quali scopi specifici (come il tracciamento dei contatti e/o la ricerca scientifica) i dati personali possono essere utilizzati, da chi e per quanto tempo possono essere conservati.

[65] Come infatti sta avvenendo in tutte le app sia in corso di realizzazione che operanti in vari Paesi.

- √ Una volta che l'epidemia si è fermata e le applicazioni di tracciamento dei contatti non sono più necessarie, è necessario predisporre una procedura per arrestare la raccolta di identificativi (disattivazione globale dell'applicazione, istruzioni per disinstallare l'applicazione, disinstallazione automatica, ecc.) Ed eliminare tutti i dati raccolti da tutti i database (applicazioni e server mobili).
- √ *Mancanza di trasparenza*

Le App di tracciamento possono raggiungere la loro massima efficienza solo se utilizzate dalla quota più ampia possibile della popolazione. La mancanza di spiegazioni su come funzionano le App di tracciamento e su come proteggono la privacy dell'utente potrebbe creare una mancanza di fiducia. Pertanto l'uso delle App di tracciamento dovrebbe essere volontario e trasparente per l'utente. Le informazioni raccolte dovrebbero risiedere sullo *smartphone* dell'utente.

- √ Per consentire a tutti gli attori coinvolti nello sviluppo e nel funzionamento delle App di tracciamento dei contatti di aderire sin dall'inizio alle leggi sulla protezione dei dati dell'UE, l'European Data Protection Board (2020) e l'European Commmission (2020) hanno pubblicato linee guida dettagliate cui attenersi.

2. Razionale scientifico e richiami tecnici.

I dettagli biologici della trasmissione del virus sono noti in termini generali: questi virus possono passare da un individuo all'altro attraverso quattro diversi percorsi di trasmissione che sono strettamente allineati alle loro implicazioni per la prevenzione:

I. *sintomatica*: diretta da un individuo sintomatico, attraverso un contatto che può essere facilmente ricostruito dal destinatario.

II. *pre-sintomatica*: diretta da un individuo che si verifica prima che l'individuo di origine manifesti sintomi evidenti.

III. *asintomatica*: diretta da individui che non manifestano mai sintomi evidenti. Ciò può essere stabilito solo dal follow-up, poiché l'osservazione di un singolo punto temporale non può distinguere completamente gli individui asintomatici da quelli pre-sintomatici.

IV. *ambientale*: tramite contaminazione, e in particolare in un modo che non sarebbe tipicamente attribuibile al contatto con la fonte in una ricognizione dei contatti (vale a dire, ciò non include le coppie di trasmissione che erano in stretto contatto, ma per chi in realtà il contagio passa attraverso l'ambiente anziché più direttamente). Questi potrebbero essere identificati in un'analisi dei movimenti spaziali.

Nel Paese in cui l'epidemia ha avuto inizio, la Cina, la lotta al Coronavirus è stata portata avanti attraverso misure di contenimento "draconiane", a partire dalla quarantena totale della città di Wuhan (con quasi 15 milioni di abitanti) e dal blocco di ogni forma di trasporto anche negli altri centri principali dello Hubei. In parallelo, il governo ha realizzato una campagna per identificare i cittadini affetti da Covid-19, attraverso un'App in grado di valutare il rischio delle persone assegnando ad ogni cittadino un diverso grado di pericolosità epidemica: una volta immessi alcuni dati, il sistema è in grado di tracciare gli spostamenti e gli incontri delle persone e assegna un codice (verde, giallo o rosso) a seconda del proprio stato di salute o rischio di infezione. Le persone non possono muoversi senza mostrare prima il codice memorizzato sull'App. Il timore è però che, superata la fase di emergenza, determinati strumenti tra cui anche i software di riconoscimento facciale, non vengano abbandonati[66].

Anche la Corea del Sud è riuscita ad ottenere risultati molto positivi grazie a diverse

[66] Cfr. L. Kuo, 'The new normal': China's excessive coronavirus public monitoring could be here to stay', The Guardian, 9 Mar 2020 in https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

applicazioni mobili, tra cui "Corona 100M", in grado di geo-localizzare gli utenti, avvisando se nel raggio di 100 metri dalla loro posizione si sia precedentemente registrata la presenza di persone contagiate da Covid-19 e in quale data[67].

Lo schema tipo di questa impostazione è il seguente:

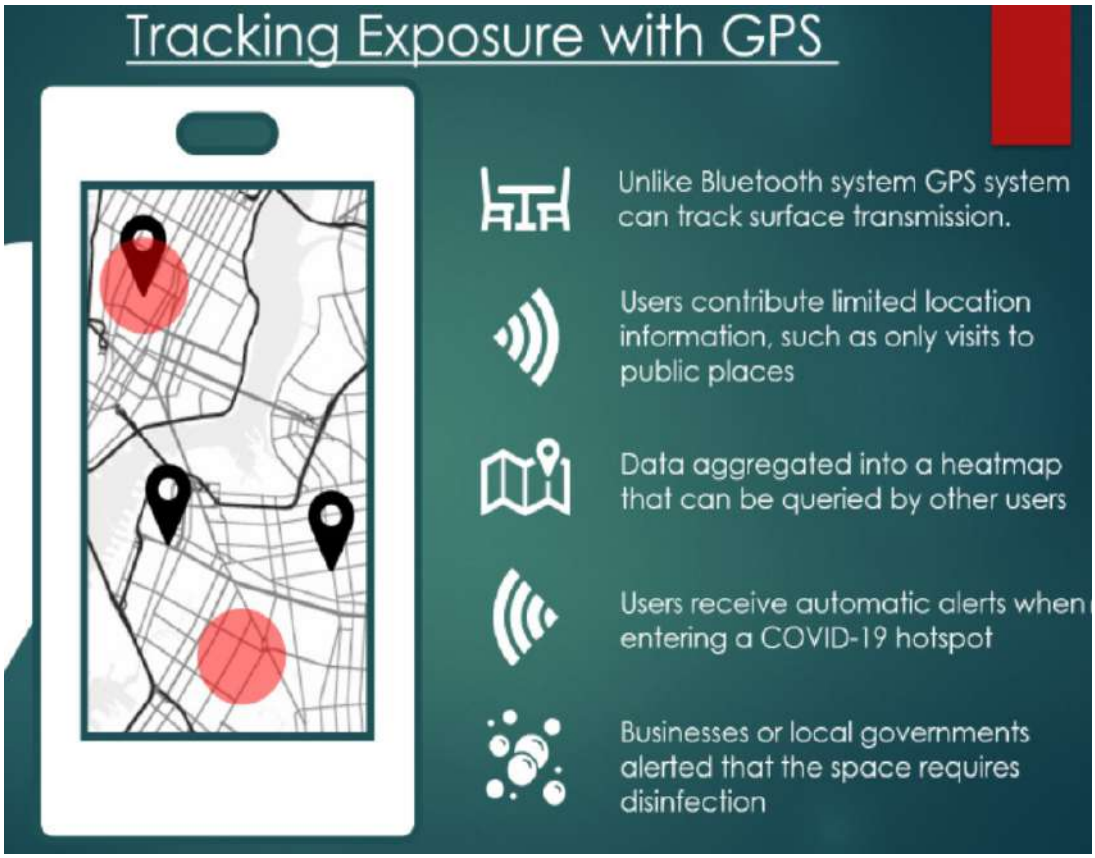


Figura 3: Metodi di tracciamento dell'esposizione con GPS (Credit: M Eifler).

Secondo qualche commentatore "si tratta, in sostanza, di un'opera ben strutturata di 'spionaggio' a tappeto degli individui realizzata grazie alla combinazione dei dati di geo-localizzazione dell'oltre un milione di utenti che ha effettuato il download dell'App, con quelli forniti dal governo"[68].

Invece di pensare a un *lockdown* di proporzioni nazionali, la Corea ha invece agito sul fronte tecnologico, attraverso la tempestiva individuazione dei soggetti positivi e la ricostruzione dei loro spostamenti. "A farne le spese la privacy, certo, ed è per questo che le misure di contenimento del virus messe in campo da Seul, in Europa hanno fatto discutere"[69].

Naturalmente, simili misure sono "agli antipodi di quanto previsto dalla normativa europea in materia di protezione e circolazione dei dati, poiché comportano un controllo 'assoluto', da parte dello Stato, dei dati personali dei cittadini – inclusi, in particolare, i dati relativi alla salute – fatti confluire in un database centralizzato e resi, in parte, accessibili agli utilizzatori delle App"[70].

---

[67] Cfr. A. Lisi, 'Coronavirus: lockdown vs. download. La privacy alla radice del contrasto della pandemia' | L'HuffPost online, 17/03/2020.
[68] Ibidem.
[69] Ibidem.
[70] Ibidem.

Tecnicamente il concetto di tracciamento dei contatti è abbastanza semplice[71]: quando si scopre che qualcuno è stato infettato da un determinato agente patogeno, si tenta di trovare tutti coloro con cui quella persona potrebbe avere avuto un contatto mentre la persona era infettiva[72]. Qualcuno infetto fornisce agli "investigatori"- che potrebbero essere medici, infermieri, volontari o studenti in medicina e infermieristica - un elenco di persone con cui è stato in contatto per un determinato periodo di tempo, di solito circa una finestra di otto giorni prima e dopo di quando hanno iniziato a mostrare sintomi. I Centri per il controllo e la prevenzione delle malattie (CDC) definiscono il "contatto" in questo caso come avvenuto a una distanza di 1,8 metri circa o meno, per 10 o più minuti[73].

Riferendosi a questa persona come caso-indice, l'App conterrebbe anche un "diario clinico" per la *early detection*, al fine di individuare precocemente le infezioni[74].

La condivisione dei dati da parte delle società tecnologiche sta aiutando i governi a combattere la vertiginosa diffusione del coronavirus monitorando il rispetto delle distanze sociali e degli ordini di restare in casa[75]. "Esiste un comprensibile desiderio di mettere insieme tutti gli strumenti a nostra disposizione per aiutare a far fronte alla pandemia", ha affermato Michael Kleinman, direttore della Silicon Valley Initiative di Amnesty International. "Tuttavia, gli sforzi dei paesi per contenere il virus non devono essere usati come una scusa per creare un sistema di sorveglianza digitale notevolmente ampliato e più intrusivo[76]".

In realtà, nuove pratiche di condivisione dei dati stanno avvenendo a molti livelli.

Google[77]ha annunciato che rilascerà nuovi dati su come la pandemia ha ridotto il traffico

---

[71] Cfr. B. Y. Lee, 'To Help Stop COVID-19 Coronavirus, What Is Contact Tracing, How Do You Do It', Apr 17, 2020 in https://www.forbes.com/sites/brucelee/2020/04/17/what-is-contact-tracing-why-is-it-key-to-stop-covid-19-coronavirus/.

[72] Tra i parametri più importanti, vi sono A) "Come le app determinano il rischio: a seconda del design dell'app, potrebbe essere possibile programmare un cut-off definito, ad esempio tutti i contatti che soddisfano le definizioni di esposizione a meno di due metri per più di 15 minuti vengono avvisati. Alcune app consentono anche di calcolare un punteggio di rischio totale in base a diverse combinazioni di tempo e distanza, in modo che un'esposizione inferiore a 15 minuti ma a distanza molto ravvicinata possa comunque attivare una notifica. Potrebbe anche esserci la possibilità di includere altri parametri per calcolare il rischio, ad esempio il giorno in cui si è verificato il contatto relativamente all'insorgenza dei sintomi nel caso. Il risultato di tale calcolo del rischio sarebbe un punteggio di rischio totale. Determinare quale sarebbe un limite adeguato per la notifica alle persone di contatto richiederà una valutazione e una calibrazione. B) Considerazioni sulla determinazione delle impostazioni: le autorità sanitarie pubbliche devono garantire che le impostazioni di tempo e distanza siano sufficientemente ampie da "catturare" i contatti più a rischio. Tuttavia, se le impostazioni sono tali che un gran numero di persone viene indicato come "contatti" e gli viene chiesto di adottare misure come l'auto-quarantena, ciò potrebbe comportare un onere per gli individui e la società e nel tempo probabilmente ridurrà l'accettabilità e l'adozione dell'app. A seconda dell'intensità del follow-up dei contatti, un gran numero di contatti aggiuntivi tracciati attraverso le app potrebbe poi comportare un onere per le autorità sanitarie pubbliche" in European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020, cit., pag.8.

[73] Cfr. anche "indagano sui contatti di Bob se hanno trascorso oltre 15 minuti insieme entro 2 metri" in T. Pueyo, 'Coronavirus: How to Do Testing and Contact Tracing', Medium 28/4/2020 in https://medium.com/@tomaspueyo/coronavirus-how-to-do-testing-and-contact-tracing-bde85b64072e, pag. 17.

[74] Cfr. A. Rahinò, 'App per tracciare i contagi: tra diritto alla salute e diritto alla privacy', 26 Marzo 2020 in https://studiolegalelisi.it/approfondimenti/app-per-tracciare-i-contagi-tra-diritto-alla-salute-e-diritto-alla-privacy/.

[75] Cfr. B. Brody, N. Nix, 'Pandemic Data-Sharing Puts New Pressure on Privacy Protections', Bloomberg Technology, 5 aprile 2020 in https://www.bloomberg.com/news/articles/2020-04-05/pandemic-data-sharing-puts-new-pressure-on-privacy-protections?srnd=technology.

[76] Ibidem.

[77] Cfr. N. Lomas, 'Google is now publishing coronavirus mobility reports, feeding off users' location history', Techcrunch, 03/04/2020 in https://techcrunch.com/2020/04/03/google-is-now-publishing-coronavirus-mobility-reports-feeding-off-users-location-history/?guccounter=1&guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8 &guce .

pedonale verso centri di transito, negozi al dettaglio e parchi pubblici in oltre 130 paesi. La società ha dichiarato di rispondere alle richieste di funzionari della sanità pubblica che vogliono sapere come le persone si spostano in città come un modo per combattere meglio la diffusione di Covid-19, la malattia causata dal virus. Google ha ribadito che, nei suoi rapporti sulla mobilità, utilizza dati anonimizzati e aggregati[78].

Apple Inc. ha lanciato la sua iniziativa[79] quando ha annunciato che "Apple ha rilasciato oggi uno strumento di tendenze dei dati sulla mobilità da Apple Maps per supportare il lavoro di impatto in corso in tutto il mondo per mitigare la diffusione di COVID-19. Questi dati sulla mobilità possono fornire utili spunti ai governi locali e alle autorità sanitarie e possono anche essere utilizzati come base per nuove politiche pubbliche mostrando il cambiamento nel volume delle persone che guidano, camminano o prendono il trasporto pubblico nelle loro comunità.

Maps non associa i dati di mobilità all'ID Apple di un utente e Apple non conserva una cronologia della posizione dell'utente. Utilizzando i dati aggregati raccolti da Apple Maps, il nuovo sito Web indica le tendenze di mobilità per le principali città e 63 Paesi o regioni. Le informazioni vengono generate contando il numero di richieste fatte ad Apple Maps per le indicazioni. I set di dati vengono quindi confrontati per riflettere un cambiamento nel volume di persone che guidano, camminano o prendono il trasporto pubblico in tutto il mondo. La disponibilità dei dati in una particolare città, paese o regione è soggetta a una serie di fattori, tra cui le soglie minime per le richieste di direzione effettuate ogni giorno.

Apple ha integrato la privacy nel nucleo di Maps sin dall'inizio. I dati raccolti da Maps, come i termini di ricerca, il percorso di navigazione e le informazioni sul traffico, sono associati a identificatori casuali e rotanti che si ripristinano continuamente, quindi Apple non ha un profilo dei tuoi movimenti e ricerche. Ciò consente a Maps di offrire un'esperienza eccezionale, proteggendo al contempo la privacy degli utenti".

Restano però indispensabili due cautele:

1) "l'importanza di applicare misure adeguate per garantire la trasmissione sicura dei dati dai fornitori di telecomunicazioni. Sarebbe inoltre preferibile limitare l'accesso ai dati agli esperti autorizzati in epidemiologia spaziale, protezione dei dati e scienza dei dati"[80].
2) "La necessità di una pronta distruzione dei set di dati al termine dell'emergenza - è un altro elemento chiave della *guidance* tecnica[81].

---

[78] Su https://www.google.com/covid19/mobility/ si legge infatti che "I rapporti sugli spostamenti della comunità sono stati sviluppati in modo da fornire informazioni utili in conformità con i nostri rigidi protocolli sulla privacy e nel rispetto della privacy degli utenti. In nessun caso vengono messe a disposizione informazioni che consentono l'identificazione personale quali posizione, contatti o spostamenti di un individuo. Le informazioni presenti in questi rapporti sono basate su set di dati aggregati e anonimizzati degli utenti che hanno attivato l'impostazione Cronologia delle posizioni, che è disattivata per impostazione predefinita. Gli utenti che hanno attivato la Cronologia delle posizioni possono decidere di disattivarla in qualsiasi momento dal proprio Account Google e possono sempre eliminare i dati della Cronologia delle posizioni dalla sezione Spostamenti. Usiamo inoltre la stessa tecnologia di anonimizzazione di altissimo livello usata quotidianamente nei nostri prodotti per mantenere privati e protetti i dati relativi alle tue attività". Infine, "questi rapporti saranno disponibili per un periodo di tempo limitato, ossia finché i funzionari della sanità pubblica li riterranno utili per la loro attività finalizzata ad arrestare la diffusione della malattia COVID-19".

[79] Cfr. Apple Newsroom, 'Apple makes mobility data available to aid COVID-19 efforts', April 14, 2020 in https://www.apple.com/newsroom/2020/04/apple-makes-mobility-data-available-to-aid-covid-19-efforts/.

[80] Cfr. N. Lomas, 'Telco metadata grab is for modelling COVID-19 spread, not tracking citizens, says EC', Techcrunch, March 27, 2020 in https://techcrunch.com/2020/03/27/telco-metadata-grab-is-for-modelling-covid-19-spread-not-tracking-citizens-says-ec/.

[81] Ibidem.

3. Centralizzazione vs. Decentralizzazione di dati e Informazioni: differenze e conseguenze su *data protection* e privacy.

Abbiamo visto come la Commissione Europea abbia chiesto un approccio comune dell'UE per rafforzare l'efficacia degli interventi digitali e garantire il rispetto dei diritti e delle libertà chiave[82].

L'organo esecutivo dell'Unione europea vuole infatti garantire che gli sforzi individuali degli Stati membri per utilizzare i dati e gli strumenti tecnologici nella lotta al COVID-19 siano allineati e 'interoperabili' e quindi essere più efficaci, dato che il virus non rispetta i confini nazionali.

Allo stesso tempo, la sua raccomandazione[83] pone un forte accento sulla necessità di garantire che i diritti fondamentali dell'UE non vengano superati nella corsa per mitigare la diffusione del virus, con la Commissione che esorta le autorità di sanità pubblica e gli istituti di ricerca a osservare il principio di minimizzazione dei dati durante l'elaborazione di dati personali per la lotta al coronavirus. In particolare, scrive che tali organismi dovrebbero applicare quelle che definisce "garanzie appropriate", elencando la pseudonimizzazione, l'aggregazione, la crittografia e il decentramento come esempi di buone pratiche.

Concettualmente, ma anche per i risvolti pratici, nell'approccio verso le App di tracciamento dei contatti del coronavirus un forte "scisma" sta continuando a dividere l'Europa [84], dove il principale punto di contesa tra i gruppi è: centralizzazione vs decentralizzazione.

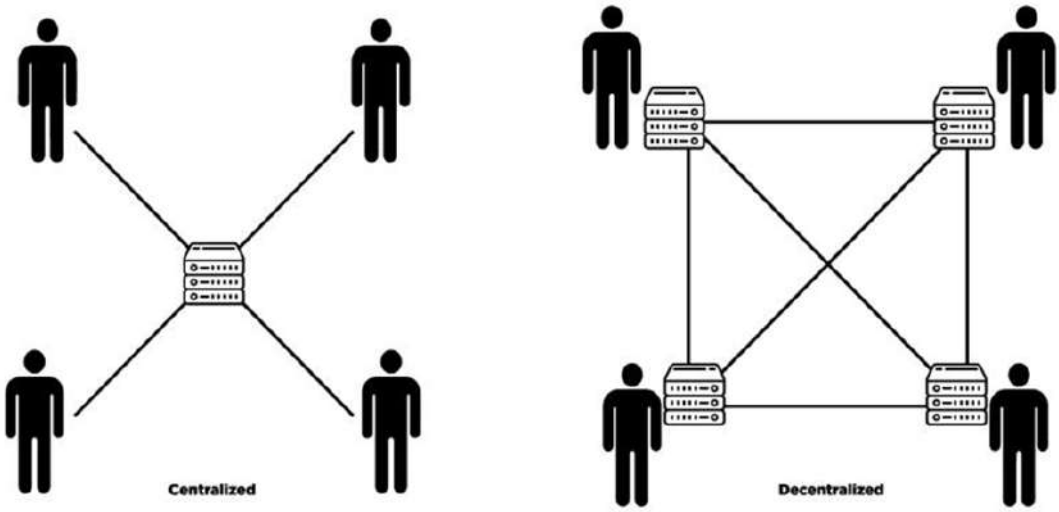


Figura 4: Impostazione centralizzata oppure decentralizzata.

Verso il lato del primo *framework* c'è un consorzio di accademici e parti interessate della *business community* che convergono sotto l'ombrello PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing). Questo gruppo ha creato una cosiddetta soluzione di

[82] Si veda anche N. Lomas, 'Call for common EU approach to apps and data to fight COVID-19 and protect citizens' rights', April 8, 2020 in https://techcrunch.com/2020/04/08/call-for-common-eu-approach-to-apps-and-data-to-fight-covid-19-and-protect-citizens-rights/.

[83] Cfr. European Commision, Recommendation C(2020) 2296 of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, cit..

[84] Cfr. L. Clarke, 'PEPP-PT vs DP-3T: The coronavirus contact tracing privacy debate kicks up another gear', 20 /04/ 2020 in https://tech.newstatesman.com/security/pepp-pt-vs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear.

tracciamento dei contatti Covid-19 "*privacy preserving*", in quanto "PEPP-PR è stato esplicitamente creato per aderire ai forti leggi e principi europei in materia di privacy e protezione dei dati", scrive il gruppo in un manifesto online[85] e uno dei suoi membri, Christophe Fraser, professore presso il Dipartimento di Medicina di Nuffield presso l'Università di Oxford, è anche coinvolto nello sviluppo dell'app NHSX del governo britannico.

Dall'altro lato c'è DP-3T[86], un gruppo di accademici attenti alla privacy che ha sviluppato una soluzione totalmente decentralizzata per il tracciamento dei contatti del coronavirus che conserva i dati sui portatili, piuttosto che inviarli a un database centralizzato gestito, ad esempio , dal servizio sanitario di un paese.

Verso la decentralizzazione sono anche Apple e Google che stanno collaborando (cfr. anche *supra*) allo sviluppo di un sistema decentralizzato per la ricerca dei contatti che potrà funzionare ininterrottamente utilizzando il *bluetooth* sui telefoni Apple e Android. Invece per le App centralizzate in grado di funzionare continuamente, un telefono dovrebbe essere lasciato sbloccato in ogni momento .

PEPP-PT ha suscitato critiche sulla sua mancanza di trasparenza e poi sono iniziate le defezioni: il professore EPFL Marcel Salathé si è dimesso dall'iniziativa, seguito rapidamente dagli istituti di ricerca KU Leuven, EPFL, ETH Zürich e CISPA. Tutti sono migrati sul progetto DP-3T.

Intanto PEPP ha pubblicato[87] su Github vari documenti sulla "architettura di protezione dei dati e sicurezza delle informazioni" per l'implementazione tedesca di PEPP-PT, che hanno chiamato NTK: l'App funziona utilizzando la funzione *Bluetooth Low Energy* (BLE) (*ut supra*) di uno *smartphone* per monitorare la vicinanza di altri telefoni. Se un utente inserisce una diagnosi di Covid-19, l'App scorre l'elenco dei contatti del telefono nelle ultime tre settimane e valuta per ciascuno un "punteggio di rischio" in base al grado e alla durata della prossimità, nonché ad altre popolazioni fattori epidemiologici di livello. Per quelli ritenuti a rischio, una notifica *push* li informa della necessità di autoisolarsi.

In termini di privacy, l'App assegna a ciascun portatile un identificatore persistente (PUID) che viene utilizzato per creare "ID effimeri"(EBID) per il portatile che cambiano periodicamente. Questi vengono creati crittografando il PUID con una chiave di trasmissione globale che viene rinnovata periodicamente. Dopo quattro settimane, la chiave viene eliminata. Sono gli EBID effimeri che vengono trasmessi dal telefono e gli EBID di altri telefoni nelle immediate vicinanze che vengono registrati. Una volta diagnosticato un paziente, con il consenso e l'autorizzazione del paziente da parte di un'autorità sanitaria, l'App carica sul server tutti gli EBID registrati nelle tre settimane precedenti, insieme all'ora del contatto, ai metadati[88] *Bluetooth* e ad altre informazioni. Il server back-end utilizza quindi le

---

[85] Pan European Privacy Protecting Proximity Tracing (PEPP-PT), 'Context and Mission' in https://404a7c52-a26b-421d-a6c6-96c63f2a159a.filesusr.com/ugd/159fc3_878909ad0691448695346b128c6c9302.pdf.

[86] Cfr. N. Lomas, 'EU privacy experts push a decentralized approach to COVID-19 contacts tracing', Techcrunch, April 6, 2020 in https://techcrunch.com/2020/04/06/eu-privacy-experts-push-a-decentralized-approach-to-covid-19-contacts-tracing/.

[87] Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) on Github in https://github.com/pepp-pt/pepp-pt-documentation/blob/master/10-data-protection/PEPP-PT-data-protection-information-security-architecture-Germany. pdf.

[88] "I metadati sono dati sui dati. In altre parole, sono le informazioni utilizzate per descrivere i dati contenuti in qualcosa come una pagina Web, un documento o un file. Un altro modo di pensare ai metadati è come una breve spiegazione o un riassunto di quali siano i dati. Un semplice esempio di metadati per un documento potrebbe includere una raccolta di informazioni come l'autore, le dimensioni del file, la data di creazione del documento e le parole chiave per descriverlo" come si legge*, inter alia*, in M. Chapple, 'What Is Metadata? Metadata is critically important for website and database management', Lifewire, January 04, 2020 in https://www.lifewire.com/metadata-definition-and-examples-1019177.

chiavi di trasmissione globali per decrittografare gli EBID, rivelando il PUID (e quindi l'identità pseudonimizzata) di tutti i dispositivi vicini alla persona infetta nell'intervallo di date specificato.

Il gruppo DP-3T ha pubblicato rapidamente un'analisi di sicurezza e privacy del documento di PEPP-PT, in cui rileva un paio di importanti divergenze nel modo in cui funzionano i due sistemi. In particolare, su DP-3T, il calcolo del rischio viene eseguito sul telefono dell'utente dell'App, anziché dal server, il che significa che i dati non devono lasciare il telefono dell'utente. In termini di problemi di privacy, DP-3T ha messo in evidenza il potenziale per il 'creep funzionale' (*function creep*[89]): ad es., se il database viene violato, l'anonimato fornito dalla rotazione degli pseudonimi viene annullato e gli individui possono essere rintracciati più facilmente. Inoltre non si può escludere il rischio di 'sorveglianza' statale.

L'analisi di DP-3T afferma infatti che, poiché l'utente *backend* crea gli identificatori effimeri, il server backend può collegare qualsiasi identificatore passato o futuro (EBID) con l'identificatore permanente (PUID). Ciò significa che il server back-end può identificare qualsiasi individuo specifico e pseudonimo. Con una piccola quantità di dati aggiuntivi –viene utilizzato l'esempio di filmati CCTV o dati di carte di viaggio intelligenti - l'identità dell'individuo potrebbe essere rivelata. Secondo il gruppo quindi esiste un elevato potenziale per il '*creep* funzionale' e la trasformazione di uno strumento di tracciamento dei contatti del coronavirus in uno strumento di sorveglianza. Il documento afferma anche che dato un EBID target (ad esempio uno raccolto dalle forze dell'ordine o in un punto di controllo del passaporto), i movimenti di un utente specifico potrebbero essere rintracciati senza accesso al database.

L'analisi sostiene inoltre che il design centralizzato di NTK consente al back-end di apprendere l'intero grafico di contatto di un individuo infetto, nonché gli incontri tra individui non infetti. Sostiene che ciò viola il principio di minimizzazione dei dati del GDPR in quanto il server back-end ha accesso a più informazioni di quelle necessarie.

Come accennavo, un altro gruppo di esperti europei in materia di privacy ha proposto un sistema decentralizzato per la tracciabilità dei contatti COVID-19 basato su Bluetooth che secondo loro offre una maggiore protezione contro l'abuso dei dati.

Il protocollo Decentralized Privacy-Preserving Proximity Tracing (DP-PPT) (cioé 'tracciamento di prossimità decentralizzato che preserva la privacy), è stato progettato da circa 25 accademici di almeno sette istituti di ricerca in Europa, tra cui l'Istituto Federale Svizzero di Tecnologia, ETH Zurigo e KU Leuven in Belgio.

Come si legge nel 'Libro bianco' che hanno pubblicato[90], l'elemento chiave è che il design prevede l'elaborazione locale della traccia e del rischio dei contatti sul dispositivo dell'utente, in base ai dispositivi che generano e condividono identificatori Bluetooth effimeri ("EphID"), come schematizzato nella seguente infografica[91]:

---

[89] "Il *'function creep*' si verifica quando le informazioni vengono utilizzate per uno scopo che non è lo scopo originale specificato. Ad esempio, un datore di lavoro può installare un sistema di sicurezza che richiede ai dipendenti di accedere o disconnettersi dal luogo di lavoro, allo scopo di impedire l'accesso non autorizzato. Tuttavia, l' organizzazione potrebbe finire per utilizzare queste informazioni sui singoli dipendenti per tenere traccia delle presenze. Questa potrebbe essere una violazione della privacy se ad es., l'organizzazione raccoglie le informazioni per tracciare la presenza dei dipendenti senza informarli dello scopo per il quale le informazioni vengono raccolte", come si legge in S. Young, 'Technology and function creep', February 22, 2018 in https://oipc.sk.ca/technology-and-function-creep-2/.

[90] Decentralized Privacy-Preserving Proximity Tracing (DP-PPT) on Github in https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

[91] L"infografica originale '*Engagement Comic*' è in https://github.com/DP-3T/documents/tree/master/public_engagement/cartoon. Questa è la versione italiana, realizzata da S. Guida e R. Serpe (*Founder* e *Co-Founder*,

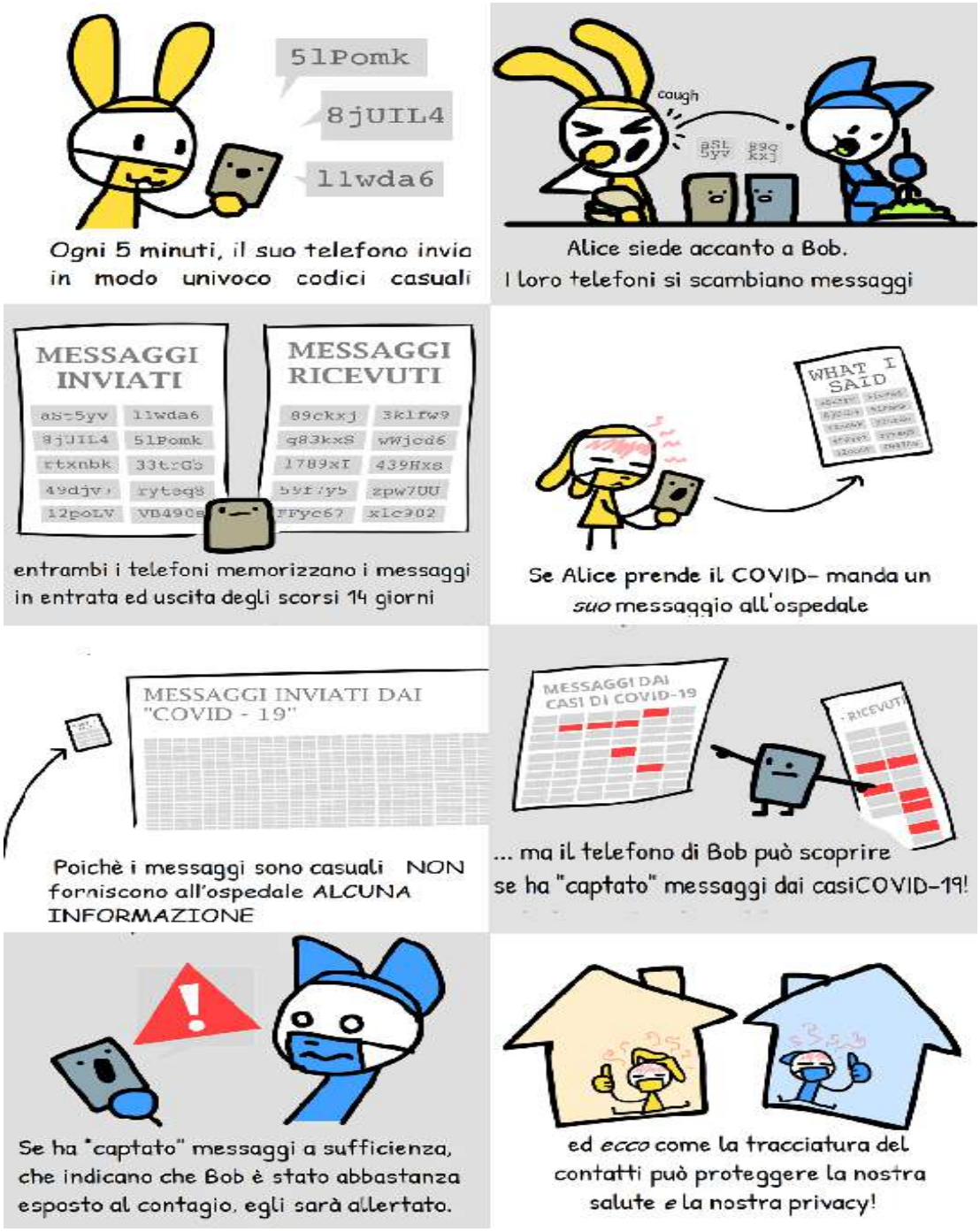


Figura 5: infografica che spiega al pubblico come funziona DP-3T (Credit: Nicky Case).

Un server back-end viene utilizzato per inviare i dati ai dispositivi, ad esempio quando una persona infetta viene diagnosticata con COVID-19, un'autorità sanitaria sancisce il caricamento dal dispositivo della persona di una 'rappresentazione compatta' (lista) di EphID nel periodo infettivo che verrebbe inviato ad altri dispositivi in modo che possano calcolare

nell'ambito della *pre-marketing strategy* relativa al progetto di 'Startup innovativa Legal Design IT Lab'), approvata e archiviata in https://github.com/DP-3T/documents/tree/master/public_engagement/cartoon/it/version_c.

localmente se esiste un rischio e avvisare l'utente di conseguenza.

In base a questo *framework* non è necessario centralizzare gli ID pseudonimizzati, in cui i dati aggregati costituirebbero un rischio per la privacy. Il che a sua volta dovrebbe rendere più semplice persuadere i cittadini dell'UE a fidarsi del sistema - e scaricare volontariamente l'app di tracciamento dei contatti utilizzando questo protocollo - dato che è progettato per resistere a eventuale riutilizzo per ipotetica 'sorveglianza' statale a livello individuale.

Il gruppo discute alcune altre potenziali minacce - come quelle poste da utenti esperti di tecnologia che potrebbero intercettare i dati scambiati localmente e decompilare / ricompilare l'app per modificare elementi - ma la tesi generale è che tali rischi sono piccoli e più gestibili rispetto alla creazione di *database* centralizzati di dati che rischiano di spianare la strada al "*creep* di sorveglianza" (*surveillance creep*)[92], vale a dire ove mai qualche Stato pensasse di utilizzare una crisi di salute pubblica come un'opportunità per creare e conservare l'infrastruttura di localizzazione a livello di cittadino.

Anche (e forse proprio per questo) la DP-PPT è stata progettata pensando allo smantellamento totale, una volta terminata la crisi della salute pubblica.

"Il nostro protocollo è una dimostrazione del fatto che sono possibili approcci rispettosi della tutela della privacy al tracciamento di prossimità e che paesi o organizzazioni non devono accettare metodi che supportano il rischio e l'uso improprio". "Laddove la legge richiede rigorose necessità e proporzionalità e il supporto della società sostiene il 'tracciamento di prossimità', questo design decentralizzato offre un modo resistente agli abusi per realizzarlo"[93].

Infine, il metodo decentralizzato (DP-3T) si adatta meglio al modello di protezione dei dati dell'UE anche con riferimento all'interoperabilità, come accennato: "i telefoni di utenti che visitano paesi stranieri, sia per lavoro che per svago, deve essere in grado di catturare i beacon dagli utenti nei paesi che visitano e includere i beacon dei pazienti con diagnosi COVID-19 in quei paesi nel loro calcolo dell'esposizione. Allo stesso modo, i residenti di un paese devono essere in grado di ricevere notifiche se a un visitatore del loro paese viene diagnosticata la COVID-19". "Tutti e tre i progetti proposti supportano l'interoperabilità tra. L'interoperabilità è possibile purché diversi operatori di diverse regioni utilizzino uno dei progetti decentralizzati proposti in questo documento"[94].

Conclusions.

"La tecnologia non tiene lontano l'uomo dai grandi problemi della natura, ma lo costringe a studiarli approfonditamente, scriveva Antoine de Saint-Exupéry"[95].

In effetti, "analizzando le azioni dei paesi dove il contagio è stato efficacemente contenuto e quelle che pensano di mettere in campo altri paesi, si capisce che la tecnologia è la chiave per realizzare soluzioni che integrino sistema sanitario, forze dell'ordine e istituzioni"[96].

---

[92] Si parla di "*surveillance creep*, quando la sorveglianza sviluppata per uno scopo limitato, come combattere una pandemia o filmare le violazioni del traffico, viene utilizzata in modi sempre più pervasivi e permanenti", come si legge in R. A. Calvo, S. Deterding, R. M. Ryan, 'Health surveillance during covid-19 pandemic. How to safeguard autonomy and why it matters', 06 April 2020, *BMJ* 2020; 369 doi: https://doi.org/10.1136/bmj.m1373.

[93] Cfr. Decentralized Privacy-Preserving Proximity Tracing (DP-PPT) on Github in https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf, cit..

[94] Ibidem.

[95] Cfr. A. Rahinò, 'App per tracciare i contagi: tra diritto alla salute e diritto alla privacy', 26 Marzo 2020 in https://studiolegalelisi.it/approfondimenti/app-per-tracciare-i-contagi-tra-diritto-alla-salute-e-diritto-alla-privacy/, cit..

[96] Cfr. M. Proverbio, 'Privacy, salute e ripresa delle attività sociali e produttive: il bilanciamento efficace che serve' - Il Sole 24 ORE, 4/4/2020 in https://www.ilsole24ore.com/art/privacy-salute-e-ripresa-attivita-sociali-e-produttive-bilanciamento-efficace-che-serve-ADwPs3H.

Ma con tutta evidenza il tema relativo al tracciamento dei contatti in relazione al suo impatto sulla privacy e sulla protezione dei dati ha anche profonde implicazioni etiche.

Da un lato, le Linee guida ECDC parlano espressamente di "*Data altruism*": come si è visto "lo scopo principale delle app è di tracciare la prossimità e avvisare le persone che sono state in contatto con persone infette al fine di rompere le catene di trasmissione. (..) Gli sviluppatori di app possono abilitare un'opzione in cui gli utenti possono acconsentire a caricare ulteriori informazioni epidemiologicamente rilevanti relative a se stessi, ad esempio l'età, alle autorità sanitarie pubbliche. Gli utenti potrebbero essere più motivati a farlo se vengono informati che il caricamento di tali dati potrebbe consentire alle autorità sanitarie pubbliche di comprendere meglio la situazione epidemiologica nel paese e le dinamiche di trasmissione. Tali dati dovrebbero essere conservati per un periodo di tempo limitato in conformità con le normative locali e dovrebbero essere garantiti sicurezza e riservatezza. Le autorità sanitarie pubbliche dovrebbero essere consapevoli di come questa richiesta sarebbe percepita dalla popolazione e se rischi di limitare l'adozione dell'app"[97].

D'altronde, come è stato autorevolmente affermato [98], "stiamo entrando in aree inesplorate dell'etica digitale. La strada da percorrere potrebbe consistere nel progettare le giuste politiche che incentivano l'adozione dell'app (volontaria, obbligatoria o una combinazione delle due) e / o in una diversa architettura dell'app (ad es. Più centralizzata, utilizzando i dati GPS ecc.) e / o la natura dell'hardware richiesto (pensa a un tracker basato su Bluetooth economico e distribuito liberamente, come quelli che puoi collegare ai tuoi tasti per trovarli a casa) e / o come viene utilizzata l'app (pensa di un hub app, in grado di supportare un'intera famiglia attraverso un solo telefono cellulare, in connessione con altri tracker Bluetooth). Ma qualsiasi soluzione dovrebbe prendersi cura delle sue implicazioni etiche ed essere abbastanza flessibile da essere rapidamente migliorata, per correggere potenziali carenze e sfruttare nuove opportunità, man mano che le pandemie si sviluppano".

E ancora "Per una volta, il problema difficile è _non privacy_. Un'app basata su Bluetooth può utilizzare dati anonimi, registrati solo nel telefono cellulare, utilizzati esclusivamente per inviare avvisi in caso di contatto con persone infette, in modo non centralizzato. Non è facile ma è fattibile. Certo, è banalmente vero che ci sono e potrebbero esserci sempre problemi di privacy. Il punto è che, in questo caso, possono essere resi molto meno urgenti rispetto ad altri problemi. Tuttavia, una volta (o, se uno è più scettico di me, anche se), la privacy è curata, altre difficoltà etiche devono essere risolte. Riguardano l'efficacia e l'equità dell'app".

Una strategia molto positiva, ancor più perché in controtendenza in un mondo ormai pervaso dal «capitalismo di sorveglianza», in cui «un altro aspetto radicale riguarda la distribuzione dei diritti alla privacy e con essa la conoscenza e la scelta". (...) In realtà, privacy e segretezza non sono opposti ma piuttosto momenti di una sequenza» [99].

Ecco perché i regolatori hanno avvertito fortemente la necessità di porre limiti alla tecnica, quella che Shoshana Zuboff ha «chiamato la dimensione materiale di potere[100] in cui sistemi impersonali di disciplina e controllo producono una certa conoscenza del comportamento umano indipendentemente dal consenso». Perciò non posso che concordare *in toto* con il nostro Garante Privacy, quando afferma che[101]"se gestita con 'metodo democratico', anche

---

[97] Cfr. European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020, cit., pag. 9.

[98] Cfr. L. Floridi, 'Mind the app - considerations on the ethical risks of COVID-19 apps', April 18, 2020 in https://thephilosophyofinformation.blogspot.com/2020/04/mind-app-considerations-on-ethical.html.

[99] Cfr.. S. Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilization', in Journal of Information Technology (2015) 30 in , https://journals.sagepub.com/doi/10.1057/jit.2015.5, pag. 82.

[100] *Ibidem*, pag. 81.

[101] Cfr. A. Soro, Presidente del Garante per la protezione dei dati personali, 'Tracciamento contagi coronavirus, ecco i criteri da seguire', in Agenda Digitale, 29 marzo 2020, riportato su sito Garante [doc. web n. 9301470].

l'emergenza può risolversi in una parentesi destinata a lasciare inalterata- persino per certi versi più forte- la nostra democrazia. La chiave è nella proporzionalità, lungimiranza e ragionevolezza dell'intervento, oltre che naturalmente nella sua temporaneità. Il rischio che dobbiamo esorcizzare è quello dello scivolamento inconsapevole dal modello coreano a quello cinese, scambiando la rinuncia a ogni libertà per l'efficienza e la delega cieca all'algoritmo per la soluzione salvifica. Così, una volta cessata quest'emergenza, avremo anche forse imparato a rapportarci alla tecnologia in modo meno fideistico e più efficace, mettendola davvero al servizio dell'uomo".

EJPLT

Immuni: inquadramento e prime considerazioni ad un mese dal via

Immuni: framing and first considerations one month from the start

SIMONA LATTE
Legal Counsel
Web Marketing Manager

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Abstract

L'adozione di Immuni da parte del Governo italiano, quale strumento attivo di lotta contro la diffusione del Covid - 19, ha suscitato e suscita diverse perplessità, in primis per quanto attiene alla tutela della privacy nonché delle libertà fondamentali. Ad un mese dal lancio dell'applicazione negli app store, tali timori sembrano riflettersi in maniera speculare nella determinazione dei cittadini italiani di scaricare l'app. Le falle di un sistema non ancora rodato emergono lasciando spazio a spunti riflessivi sulla necessità di apportare correttivi capaci di rendere questo sistema più efficiente e meritevole di fiducia.

…

The adoption of Immuni by the Italian government, as an active tool in the fight against the spread of Covid - 19, has raised, and still raises, several concerns, primarly regarding the protection of privacy and fundamentals freedoms. A month after the launch of the application in the app stores, these fears seems to be mirrored in the determination of Italian citizens to download the app. The flaws of a not yet run-in system emerge, leaving room for reflective ideas on the need to make corrections capable of making this system more efficient and worthy of trust.

Keywords: Immuni - privacy - falsi positivi.

Summary: Introduction. – 1. Il contesto. – 1.1. Prime considerazioni ad un mese dal via. – 2. Il fondamento normativo e l'informativa. – 2.1. Requisiti che ex art. 6 d.l. 28/2020 l'App Immuni deve rispettare e informativa. – 2.2. La base giuridica del trattamento. – 3. Il funzionamento di Immuni. – Conclusions.

Introduction.

L'emergenza Covid - 19 richiede un fortissimo sforzo da parte dei Governi per combattere la diffusione del virus. Si è giunti alla conclusione secondo la quale la tecnologia può essere un valido alleato al fine della gestione di questa crisi, del controllo dell'evoluzione del contagio e per lo studio del comportamento del virus stesso. Si è così prospettata la possibilità di utilizzare sistemi di tracciamento per controllare l'andamento della propagazione del Covid - 19 e scongiurare l'insorgere di nuovi focolai. Tali sistemi rischiano, tuttavia, di ledere i diritti dei cittadini, con particolare riferimento alla privacy ed è proprio questo il principale aspetto critico che è emerso nel dibattito su Immuni, l'app di contact tracing sviluppata per fronteggiare la diffusione del virus in Italia.

1. Il contesto.

Di fronte alla pandemia da Covid-19, gli Stati colpiti hanno dovuto predisporre misure di contenimento della diffusione del virus, come il distanziamento sociale.

Quasi "naturalmente", in risposta alle esigenze di controllo e previsione circa la possibile ulteriore propagazione del contagio, si è presa in considerazione la possibilità di trasporre nei paesi europei, secondo canoni rimodulati e democraticizzati, sistemi di tracciamento della diffusione del virus ispirati a quelli utilizzati nei paesi che per primi lo hanno fronteggiato e che si basano sulla raccolta di dati personali attraverso tecnologie apposite, quali ad esempio app di contact tracing.

L'Italia ha optato per l'uso di Immuni, un'applicazione che sfrutta la tecnologia bluetooth low energy creata da Bending Spoons, società milanese molto affermata nel settore della realizzazione di app e software, il cui progetto, in risposta alla fast call del Ministero dell'Innovazione, è stato selezionato tra trecento altre proposte dal Gruppo di lavoro data driven.

Tale app è in grado di contribuire all'individuazione di soggetti che potrebbero essere infetti non appena si verifichi l'evento potenzialmente contagioso, così da evitare l'ulteriore trasmissione del virus da parte di chi sia ignaro di esserne venuto in contatto.

Chiaramente, l'ipotesi del ricorso ad un modello di contenimento che si basi sulla capacità di un sistema informatico di ricostruire e, in un certo senso, "predire" il percorso della propagazione del virus da una persona all'altra, ha destato diverse perplessità, ampiamente discusse in dottrina, sotto il punto di vista della conformità alla normativa posta a tutela della privacy, quale baluardo contro potenziali discriminazioni ed abusi.

1.1. Prime considerazioni ad un mese dal via.

Ad un mese dal lancio di Immuni sugli app store, diverse sono le perplessità sul suo effettivo virtuoso funzionamento in assenza di una massiva adesione al programma e di un sistema di screening coerente, uniforme e certo, nei tempi e nelle modalità, dei soggetti che segnalino di aver ricevuto la notifica di contatto con un soggetto Covid positivo.

Il download dell'app è, come richiesto anche dall'art. 6 del D.L. 28/2020, una scelta volontaria, ma parte della dottrina ritiene che, in realtà, in alcuni casi, non scaricarla – e in buona sostanza anche non condividere col sistema Immuni, una volta accertata la propria positività al virus e ove usata l'app nei giorni precedenti l'accertamento della stessa, le proprie chiavi TEK (per la descrizione del sistema v. par. 3) che consentono di allertare le persone con cui si siano avuti contatti a rischio – potrebbe ingenerare, in capo a chi provocasse a causa di ciò un danno, pur avendo a disposizione uno strumento tecnologico tutto sommato "blando" come Immuni da poter usare per evitarlo, una responsabilità fondata su un comportamento colposo da valutarsi alla stregua del canone dell'ordinaria diligenza[1]. Tale dottrina sembrerebbe altresì velatamente auspicare un'obbligatorietà dell'applicazione che si fonderebbe sui principi espressi dagli artt. 2 e 32 della Costituzione (dovere di solidarietà e tutela della salute collettiva).

I numeri, in ogni caso, sembrano rappresentare chiaramente la sfiducia degli italiani circa l'uso di Immuni: la ministra dell'innovazione Paola Pisano a fine giugno ha dichiarato alle telecamere di SkyTg24, infatti, che i download sono stati circa quattro milioni, un numero esiguo rispetto alle aspettative e che fornisce ulteriori spunti di riflessione sul sistema elaborato per ridurre i contagi da Covid.

---

[1] A. GAMBINO si è espresso in tal senso nelle conclusioni del convengo dal titolo *I diritti audiovisivi nello sport. Quali regole tra cronaca, spettacolo e difficili equilibri economici,* Università Sapienza di Roma, 19 giugno 2020, in tal senso cfr. http://www.askanews.it/cronaca/2020/06/19/app-immuni-gambino-in-molti-casi-scaricarla-è-un-obbligo-pn_20200619_00176/

Il Commissario straordinario per l'emergenza Covid ha affermato che la principale delle ragioni per cui questo è successo «ha a che fare con la fase del ciclo di vita dell'epidemia che stiamo vivendo, che trova una qualche forma comprensibile, ma non condivisibile, di rilassamento generale[2]»

Sebbene questa sia la posizione del Commissario che sicuramente si rivela condivisibile, appare opportuno soffermarsi anche su aspetti che si intersecano con la percezione dell'efficacia e della sicurezza del sistema Immuni.

Colui che non scarica l'app è probabilmente disorientato da uno stato di carenza rispetto ad una informazione da parte delle istituzioni più chiara e mirata a contrastare le notizie che alimentano la disinformazione sull'argomento, ma anche perché teme una lesione dei propri diritti ed una limitazione delle proprie libertà, in assenza di una segnalazione da parte dell'app che indichi in maniera certa l'avvenuto "contatto a rischio" con un soggetto positivo al virus.

Ci si chiede, tuttavia, se tali timori siano fondati e se sì in che misura.

Non sono mancati, invero, casi di cronaca che hanno contribuito a gettare un'ombra sulla capacità di Immuni di segnalare i contatti effettivamente pericolosi, contribuendo a rafforzare il convincimento diffusosi sull'inefficacia e, anzi, dannosità dello strumento.

Ormai è noto il caso della donna di Bari[3] che, dopo aver ricevuto la notifica di esposizione da parte di Immuni ed averlo comunicato al proprio medico di base, è stata costretta all'autoisolamento per quindici giorni senza essere sottoposta a tampone per accertare con celerità l'effettiva positività.

La donna lamenta un malfunzionamento dell'app che avrebbe segnalato un "falso positivo" ed una mancata celere assistenza sanitaria che le consentisse di dimostrare di essere sana e, quindi, evitare l'inutile quarantena.

In realtà, anche sul sito e sull'app di Immuni viene chiarito che il sistema di contact tracing ha dei limiti tecnici e che l'app potrebbe segnalare "falsi positivi" (nel senso che, chi ricevesse una notifica di avvenuto contatto potrebbe in realtà non aver avuto un "contatto a rischio"[4] con un Covid positivo, pur tuttavia essendo stato comunque in sua prossimità per un tempo superiore ai quindici minuti).

In altre parole, essendo la tecnologia bluetooth low energy in grado di calcolare solo una stima della distanza tra i dispositivi, potrebbero essere segnalati casi di contatto a rischio anche in assenza di un effettivo contatto classificabile come tale, in presenza, cioè, di un contatto con soggetto Covid positivo ma non classificabile tra quelli la cui vicinanza è da notificare perché potenzialmente contagiosa.

A tal riguardo è il Garante stesso ad affermare la necessità che «gli utenti siano adeguatamente informati in ordine alla possibilità che l'app generi notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio…»[5], puntualizzazione che, in

---

[2] Per le dichiarazioni rese in tal senso dal Commissario Arcuri, v. *Coronavirus, Arcuri: "L'app Immuni non ha raggiunto il target, utile in autunno",* in TGCOM24, in https://www.tgcom24.mediaset.it/cronaca/coronavirus-arcuri-lapp-immuni-non-ha-raggiunto-il-target-utile-in-autunno_20480723-202002a.shtml, 9 luglio 2020.

[3] V. caso della donna "prigioniera" in casa a seguito della segnalazione da parte di Immuni dell'avvenuto contatto con soggetto Covid positivo. SECLì, *Bari «prigioniera» di Immuni: «Costretta alla quarantena dall'app, ma non mi fanno il tampone»,* in La Gazzetta del Mezzogiorno, in https://www.lagazzettadelmezzogiorno.it/news/bari/1230324/bari-prigioniera-di-immuni-costretta-alla-quarantena-dall-app-ma-non-mi-fanno-il-tampone.html, luglio 2020.

[4] Si chiarisce che il contatto che il sistema di Immuni rileva come potenzialmente a rischio e tale da dover essere segnalato all'interessato è il contatto con soggetto Covid positivo avvenuto ad una distanza inferiore ai due metri e per un tempo di permanenza superiore ai quindici minuti. V. la sezione "domande" in https://www.immuni.italia.it/faq.html

[5] Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid 19 - App Immuni - 1° giugno 2020 [9356568] del Garante per la Protezione dei Dati Personali, in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9356568

effetti, come detto, sul sito web e sull'app di Immuni viene proposta agli interessati nella sezione "domande", nella misura in cui si informa sul fatto che la stima della distanza tra dispositivi non può essere precisa e che l'app non può garantire con assoluta certezza il calcolo della distanza necessaria ai fini dell'eventuale attivazione della notifica.

Il Garante, a tal proposito infatti chiarisce che: «occorre considerare che la valutazione della distanza tra dispositivi è intrinsecamente suscettibile di errori in quanto l'intensità del segnale bluetooth dipende da fattori diversi come l'orientamento reciproco di due dispositivi o la presenza di ostacoli fra essi (compresa la presenza di corpi umani), potendo così rilevare "falsi positivi" e "falsi negativi".

Peraltro, la mancata conoscenza del contesto in cui è avvenuto il contatto stretto con un caso accertato Covid-19 (dato certamente rilevante, invece, ai fini epidemiologici, anche in ragione dell'eventuale utilizzo di sistemi di protezione) è suscettibile di creare potenzialmente numerosi "falsi positivi".

È importante infatti sottolineare che l'individuazione dei contatti a rischio è effettuata in modo probabilistico al fine di allertare gli utenti di un possibile rischio di contagio; per cui deve essere chiaro che in nessun caso la ricezione di un messaggio di allerta proveniente dall'app significa automaticamente che l'utente è stato sicuramente contagiato»[6]

Esperienza similare a quella della donna di Bari si sarebbe verificata anche in altri paesi in cui, anzi, la portata dell'errore commesso dall'app sarebbe stata molto più ampia: quasi dodicimila israeliani, infatti, sarebbero stati costretti alla quarantena a causa di un errore di calcolo sulle distanze tra dispositivi sui quali era stata installata un'applicazione di tracciamento, basata su un sistema fornito dallo Shin Bet (servizi segreti israeliani), per combattere la diffusione del Covid - 19[7]. Attualmente il sistema, che si avvale dell'app"HaMagen"[8], basato su tecnologia GPS (diversamente dall'App Immuni) presenterebbe addirittura ancora più inconvenienti rispetto alle app di contact tracing basate su bluetooth low energy e per tale motivo sarebbe passibile di incorrere in falsi positivi[9] molto più facilmente (si pensi all'imprecisione del GPS in luoghi chiusi).

Vale qui considerare come, in mancanza della possibilità di ovviare a questi inconvenienti dovuti ai limiti delle tecnologie messe in campo, sia fondamentale ed opportuno predisporre un sistema di gestione di verifica rapida "offline" dei casi di soggetti che abbiano ricevuto la notifica di esposizione e che consenta, così, di minimizzare l'impatto sulla vita privata e la libertà di movimento, al fine cioè di non sottoporre a quarantena forzata soggetti che di fatto non hanno avuto un contatto a rischio, evitando di arrecare un danno a persone che vedrebbero limitata ingiustamente e senza reale necessità la propria libertà di movimento.

2. Il fondamento normativo e l'informativa.

La *conditio sine qua non* in base alle quale è possibile somministrare Immuni è la preventiva, chiara e completa informazione degli utenti circa le finalità e le modalità di trattamento dei dati personali raccolti.

La necessità di sottoporre all'utente l'informativa prima di attivare Immuni è espressa a chiare lettere dal dato normativo che pone le linee guida per l'uso di Immuni: l'art. 6 del D.L.

---

[6] Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid 19 - App Immuni - 1° giugno 2020 [9356568] del Garante per la Protezione dei Dati Personali, in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9356568

[7] *Israele, migliaia in quarantena per errore,* in Adnkronos, in https://www.adnkronos.com/fatti/esteri/2020/07/14/israele-migliaia-quarantena-per-errore_fi9lBUj8FLd1oDNO3apdNI.html

[8] *Hamagen privacy policy*, in https://govextra.gov.il/ministry-of-health/hamagen-app/Privacy-policy-EN

[9] . T. A. ALTSHULER, R. A. HERSHKOWITZ, *How Israel's Covid -19 mass surveillance operation works,* in https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/

28/2020 (decreto convertito con legge del 25 giugno 2020, n. 70)[10]. Tale disposizione costituisce il fondamento normativo per l'implementazione del Sistema di allerta Covid - 19, vale a dire del sistema nazionale di tracciamento digitale dei contatti.

Con l'art. 6 del D.L. 28/2020 si dispone la creazione di una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, al fine di essere avvertiti in caso di contatto con soggetti infetti dal virus Sars-CoV-2, su base volontaria hanno installato sul proprio smartphone l'app Immuni.

Si tratta della norma in base alla quale è legittimo il trattamento, ex art. 2-ter del D.Lgs. 196/2003.

Il primo giugno, inoltre, il Garante per la Protezione dei Dati Personali ha adottato un provvedimento di autorizzazione all'adozione di Immuni[11], pur manifestando alcune perplessità circa alcuni aspetti, ad esempio in merito ai limiti sulla valutazione da parte dell'app della precisa distanza tra i dispositivi degli utenti che entrino tra di loro in contatto.

2.1. Requisiti che ex art. 6 d.l. 28/2020 l'App Immuni deve rispettare e informativa.

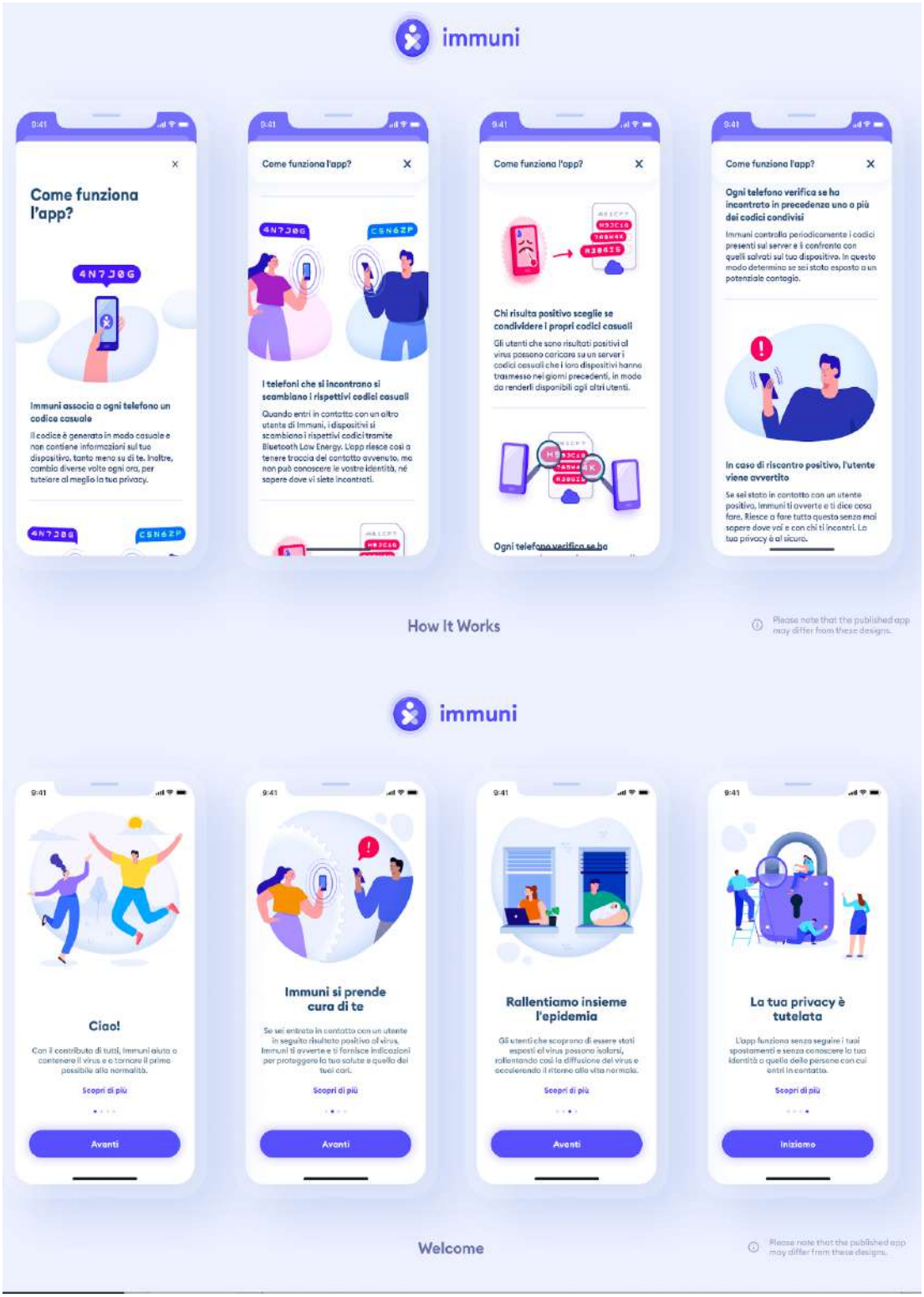
La menzionata norma pone una serie di condizioni che l'applicazione deve rispettare ai fini della propria compliance alla normativa in materia di protezione dei dati personali e in particolare prevede, al comma 2 lett. a) b) c) d) e) che:

A) gli utenti ricevano, prima dell'attivazione dell'applicazione, ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679, un'informativa chiara che definisca finalità, modi e tempi del trattamento. Tale previsione si realizza in una serie di informazioni fornite dal "sistema Immuni" sia sul sito web istituzionale, dove è possibile acquisire informazioni sulle finalità, le modalità, e i meccanismi di trattamento, nonché all'interno della stessa app, dove l'utente viene informato dapprima, al momento del download, attraverso delucidazioni generiche sul funzionamento dell'applicazione stessa corredate da infografiche (come auspicato dal Garante), nonché attraverso la somministrazione all'utente dell'informativa estesa, raggiungibile attraverso un link[12].

[10] D.L. 30 aprile 2020, n. 28 *Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19* in https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2020-04-30;28!vig=

[11] Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid 19 - App Immuni - 1° giugno 2020 [9356568] del Garante per la Protezione dei Dati Personali, in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9356568

[12] *Informativa Privacy*, https://www.immuni.italia.it/app-pn.html



B) i dati personali raccolti siano, in ossequio al principio di minimizzazione «esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19 […] nonché ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti». A tal riguardo, l'informativa chiarisce che i dati raccolti appartengono a tre categorie:

- Elenco A), valido per tutti gli utenti che usano Immuni. In questo elenco rientrano: 1) dati relativi alla provincia di domicilio (indicata dall'utente in fase di attivazione dell'app), usati per consentire di monitorare lo sviluppo dell'epidemia; 2) indicatori di corretto funzionamento per verificare e consentire il corretto funzionamento dell'app; 3) token temporanei per validare il funzionamento degli indicatori di corretto funzionamento; 4) indirizzo IP necessario per far comunicare server ed app. I tempi di conservazione di questi dati sono: per i numeri 1) e 2) fino alla fine dell'emergenza e comunque non oltre il 31 dicembre 2020; per il numero 3) fino a due mesi; per il numero 4) non viene conservato nell'ambito del sistema Covid - 19.
- Elenco B), è invece costituito dai dati aggiuntivi a quelli sopra indicati che vengono trattati per i soli utenti esposti al rischio di contagio e sono: 1) ricezione della notifica di esposizione per consentire di stimare quanti utenti vengono avvertiti dall'app e predisporre iniziative e risorse per prendersi cura degli utenti che hanno ricevuto la notifica.; 2) data dell'ultimo contatto a rischio per stimare entro quanto tempo potrebbero manifestarsi i sintomi e predisporre le iniziative necessarie per prendersi cura dei soggetti avvertiti del rischio. Tali dati vengono conservati fino alla cessazione dello stato di emergenza e comunque non oltre il 31 dicembre 2020.
- Elenco C), è infine l'elenco dove si indicano i dati raccolti per i soli utenti risultati positivi al virus Covid 19 ed è costituito da: 1) chiavi TEK con cui il dispositivo dell'utente ha generato i codici RPI temporanei nei 14 giorni precedenti (v.paragrafo). Queste chiavi vengono conservate per 14 giorni.; 2) indicatori di rischio di precedenti contatti per stimare il livello di rischio del contatto avvenuto con un altro soggetto positivo. Tali indicatori servono a migliorare l'algoritmo e a renderlo più efficiente nella valutazione di rischio concernente il contatto con soggetto positivo. Tali dati vengono conservati fino alla cessazione dello stato di emergenza e comunque non oltre il 31 dicembre 2020; 3) codice OTP costituito da una combinazione di 10 caratteri che verranno dettati dal soggetto risultato positivo al Covid 19 all'operatore sanitario affinché l'utente possa infine caricare le proprie chiavi TEK nel sistema. Tale codice resta memorizzato per 2 minuti e 30 secondi.

C) il trattamento deve essere effettuato sulla base dell'utilizzo di dati di prossimità dei dispositivi, resi anonimi o pseudonimizzati (v. par. 3) ed è esclusa in ogni caso la geolocalizzazione dei singoli utenti. Questa la caratteristica principale dell'app Immuni che non consente di localizzare a livello geografico la posizione degli utenti, tenendo al sicuro l'utente rispetto ad azioni di identificazione che potrebbero sfociare in discriminazioni e violazione dei diritti. Tale indicazione viene fornita anche nell'informativa breve dove si offrono sommarie indicazioni sul funzionamento dell'app prima che l'utente acceda alla fase di attivazione vera e propria e prima che spunti la casella dove si dichiara di aver letto l'informativa privacy estesa (raggiungibile, come già sottolineato, tramite apposito link a fianco alla casella).

D) garantire misure che assicurino la sicurezza e la disponibilità del sistema di trattamento e che evitino la possibilità di una re-identificazione degli interessati. Tutto il sistema di Immuni è pensato per evitare e non consentire la re-identificazione degli utenti, benché di fatto questo non sia tecnicamente impossibile ricorrendo una serie di circostanze e fattori.

E) indicazione dei tempi di conservazione dei dati, tempi che devono essere limitati. Come messo in evidenza, per ciascuna tipologia di dato è indicata un preciso limite temporale di conservazione che comunque non può superare il 31 dicembre 2020.

Dalla lettura dell'informativa sembra, dunque, evidente lo sforzo profuso dalle istituzioni di rispondere da un lato all'esigenza di tutelare la salute pubblica attraverso l'app, dall'altro di

predisporre un sistema trasparente in grado di tutelare la privacy degli utenti che aderiscano, pur essendo indubbi, come evidenziato anche dal Garante nel provvedimento menzionato, e non esclusi in assoluto i rischi di re-identificazione, anche in maniera indiretta, dei soggetti che avessero segnalato la propria positività al sistema.

2.2. La base giuridica del trattamento.

Esclusa l'ipotesi della raccolta del consenso per il trattamento dei dati acquisiti da Immuni (ma non la volontarietà sull'utilizzo dell'app e su ogni fase relativa al sistema di tracciamento), dalla lettura dell'informativa sulla privacy cui l'app rinvia prima di poter procedere alla sua attivazione, emerge che la base giuridica per la quale si è optato è individuata nell'interesse pubblico in base agli artt. 6 par. 2 let. e) e 9 par. 2 lett. i) e j) del GDPR nonché agli artt. 2-ter e 2-sexies del Codice in materia di Protezione dei Dati Personali (D.Lgs.196/2003 e s.m.i.).

Questo vuol dire che il Titolare del trattamento (il Ministero della Salute) è legittimato al trattamento dei dati in ragione della seguente necessità:

- esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6 par. 2 let. e) del GDPR)*;*

Inoltre, l'informativa richiama il ricorrere delle eccezioni di cui all'art. 9 par. 2 lett. i) e j) del GDPR che escludono l'applicabilità del generale divieto, previsto al paragrafo 1 dello stesso articolo, di trattamento dei dati relativi alla salute.

In base a questa disposizione il par. 1 dell'art. 9 non si applica quando si verifichino, tra l'altro, i seguenti casi:

- il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero […](art. 9 par 2 let. i));
- il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici […] (art. 9 par.2 let. j)).

Questa scelta, tuttavia, è soggetta a critica da una parte della dottrina in quanto la base giuridica per il trattamento dei dati finalizzato ad «allertare gli utenti che hanno avuto un contatto a rischio con altri utenti risultati positivi al SARS-CoV-2 (il virus che provoca il Covid-19) e tutelarne la salute […]» sarebbe identificabile non già nell'ipotesi di cui all'art. 6 par. 2 let. e) del GDPR, bensì in quella ex art. 6 par. 2 let. b) applicabile quando «il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte […]». Una volta scaricata l'app l'utente la utilizza per ottenere una prestazione in suo favore che è quella di essere avvertito nel caso venisse in contatto con un soggetto positivo al virus SARS-CoV-2.

Diversamente, per quanto attiene al trattamento dei dati in forma aggregata per fini statistici e sanitari sarebbe stata ben identificata la base giuridica come indicato nell'informativa.

3. Il funzionamento di Immuni.

Si rileva che nell'informativa, come già anticipato dal Garante nel provvedimento di autorizzazione citato, si afferma che il Titolare del trattamento dei dati raccolti nell'ambito del Sistema di allerta Covid - 19 è il Ministero della Salute.

Inoltre, all'interno di tale documento viene spiegata sinteticamente la modalità di flusso dei dati raccolti durante il funzionamento dell'applicazione.

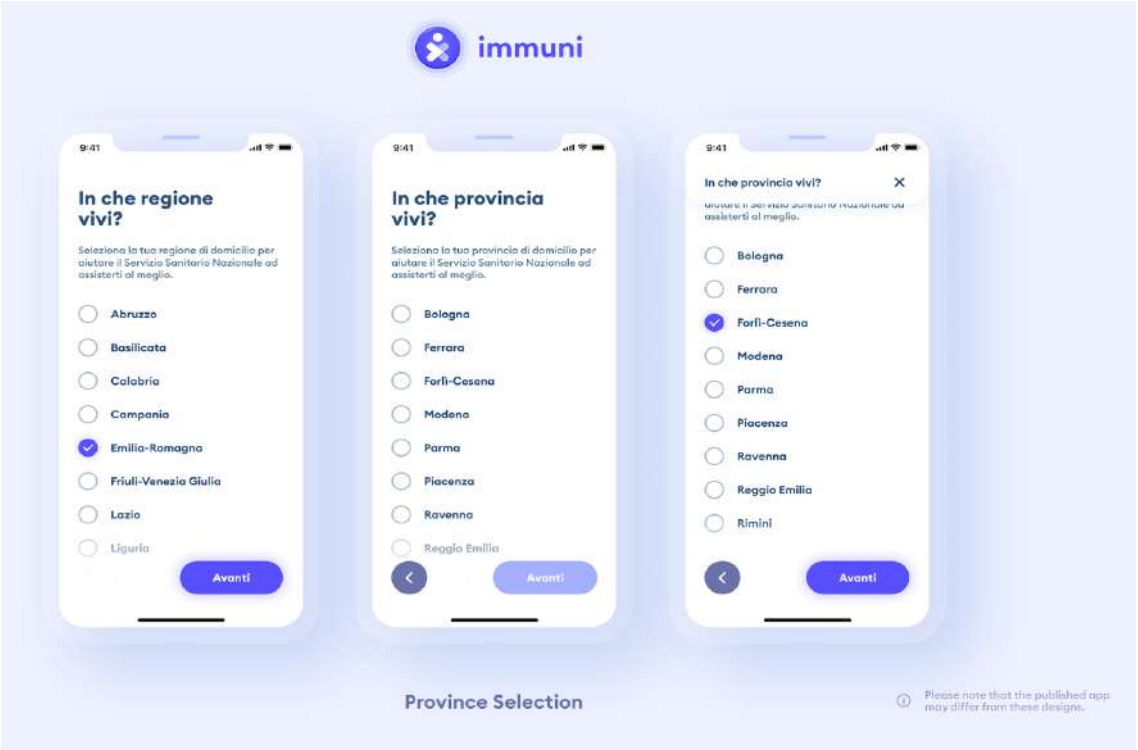
Si chiarisce sul sito web istituzionale di Immuni e sull'app, una volta completata la procedura di attivazione, che l'infrastruttura informatica che è stata scelta per raccogliere i dati dalla piattaforma collegata all'app Immuni - disponibile per il download dal 1 giugno - è situata in Italia. Essa è gestita dalla società pubblica SoGEI S.p.a. (Società Generale

Informatica), controllata dal Ministero dell'Economia e delle Finanze (nel contesto di Immuni gestisce i server).

SoGEI e il Ministero dell'Economia e delle Finanze operano dunque in qualità di Responsabili del trattamento.

A seguito del coinvolgimento e di una cooperazione sinergica tra Apple e Google si è resa possibile l'operatività dell'app anche a schermo inattivo e si è potuto optare per un sistema di tracciamento tramite una versione della tecnologia bluetooth (bluetooth low energy) che raccoglie i dati in modo decentralizzato peer to peer (Decentralised Privacy-Preserving Proximity Tracing) «in un'area crittograficamente protetta»; l'app quindi non sfrutta la tecnologia GPS e non effettua geolocalizzazione.

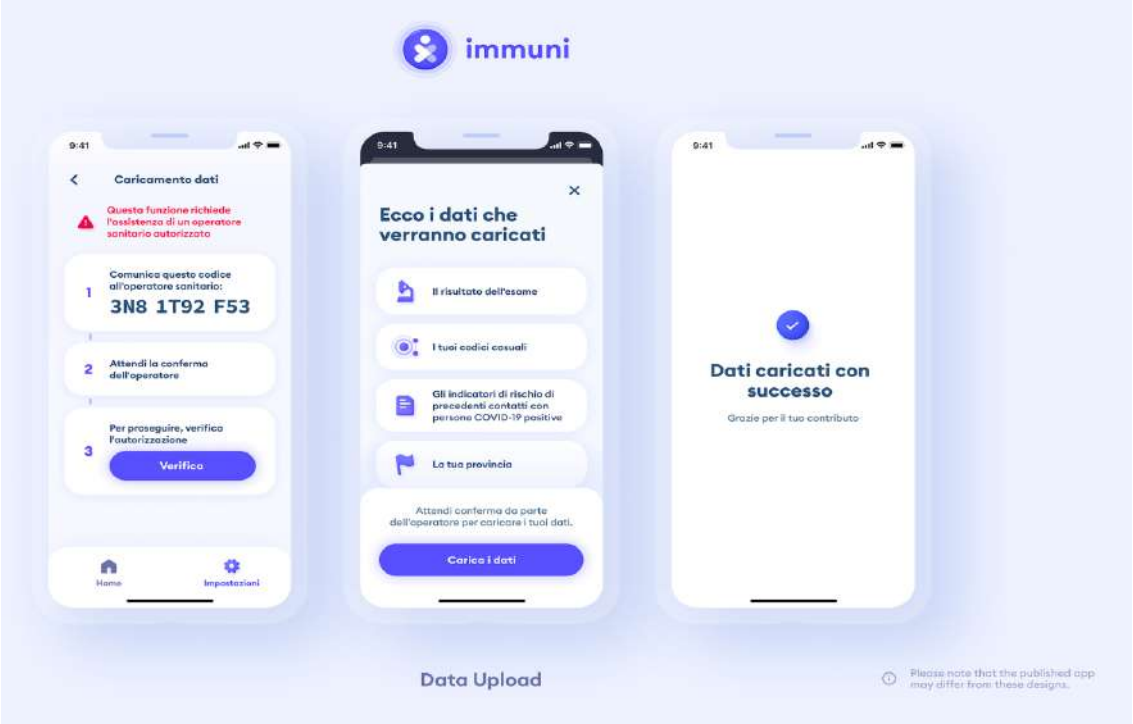
Una volta scaricata, l'applicazione chiede all'utente di dichiarare di avere almeno 14 anni e gli somministra attraverso un link l'informativa, chiede poi la regione e la provincia di domicilio, infine chiede l'accesso all'uso del bluetooth e, per i soli dispositivi Android, anche l'attivazione della geolocalizzazione che non viene tuttavia usata da Immuni ma serve affinché il sistema operativo possa rilevare i dispositivi bluetooth vicini.



Prima di essere completamente operativa, l'app richiede ancora una volta se si desidera attivare le notifiche di esposizione al COVID-19, chiarendo di nuovo la propria funzione indicatrice di eventuali contatti con persone risultate positive al test del Covid-19 e che «dati sulla data, la durata e l'intensità del segnale associati all'esposizione verranno condivisi con l'app».

Ogni giorno l'app genera una chiave alfanumerica composta da 128 bit, c.d. TEK (Temporary Exposure Key) in base alla quale l'app crea un codice identificativo c.d. RPI (Rolling Proximity Identifier) che viene emesso dallo smartphone tramite bluetooth per 10 minuti. Questo vuol dire che questo codice ID viene modificato ogni 10 minuti dalla chiave TEK nota solo all'app.

Se due smartphone su cui è attiva Immuni entrano l'uno nel raggio d'azione dell'altro, i



due device registreranno reciprocamente le RPI che in quel momento stanno operando, la distanza tra i due dispositivi e i tempi di permanenza. Sia le TEK che gli RPI vengono cancellati dal dispositivo ogni 14 giorni. Gli ID con cui si è venuti in contatto resteranno così memorizzati nell'app e non verranno comunicati esternamente a nessuno.

Ma come fa quindi il sistema centrale a notificare ai singoli soggetti che si è venuti in contatto con una persona risultata positiva al test Covid-19?

Qui sopraggiunge l'intervento dell'operatore umano: «il funzionamento dell'app deve essere seguito da altri strumenti, come i test diagnostici e soprattutto da interventi di operatori del sistema sanitario, anche per consentire la tracciabilità manuale dei contatti al fine di eliminare i casi dubbi […] In questo modo si eviterebbe la soggezione a decisioni esclusivamente automatizzate, interamente affidate all'algoritmo, come richiesto dall'art. 22 del GDPR, consentendo la correzione di possibili imprecisioni e storture, dal rilevante impatto sulla salute e sulla libertà dei singoli, dovute all'impiego di informazioni inesatte[13]».

Quando una persona risulti positiva al Covid-19 l'operatore sanitario appositamente autorizzato chiede a chi abbia già scaricato ed attivato Immuni se acconsente all'utilizzo dell'informazione concernente la sua positività ai fini della notifica alle persone entrate in contatto con lei, gli chiede cioè di rendere disponibili le sue chiavi TEK (È sotto questo punto di vista che, come anticipato, si prospettano scenari di possibile responsabilità per coloro che omettano la comunicazione delle proprie TEK. Pur essendo assodato il canone della volontarietà lungo tutta la filiera dei dati raccolti dal sistema Immuni, soprattutto in alcune circostanze ed in alcuni contesti, non scaricare Immuni e non comunicare le TEK potrebbe realmente costituire un'ipotesi di responsabilità sanzionabile).

Se questa persona accetta, l'operatore chiede all'utente di aprire la propria app e di generare un codice OTP (One Time Password) che dovrà comunicare all'operatore e attende poi l'autorizzazione per effettuare l'upload delle TEK. L'operatore, attraverso il Sistema TS, inserisce il codice OTP comunicatogli dall'utente e la data di inizio dei sintomi trasmettendo tali informazioni al sistema di backend di Immuni e, da quel momento, il soggetto i cui dati vengono trattati avrà circa 2 minuti per cliccare sul tasto "Verifica" all'interno dell'app Immuni che ha sul proprio smartphone per completare l'upload delle sue TEK nel sistema.

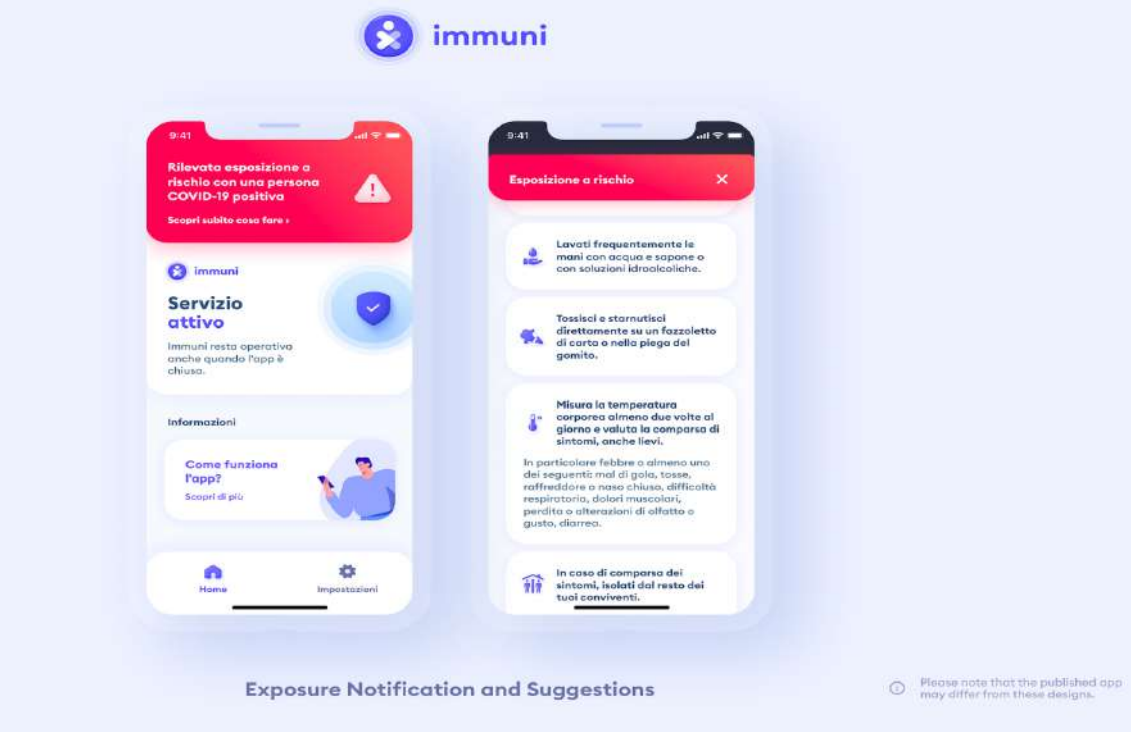
Questa operazione consente di verificare la corrispondenza tra il codice inserito

[13] D. POLETTI, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza,* in Persona e Mercato, 2020, fasc. n. 2., 31 - 76.

dall'operatore sanitario e le chiavi alfanumeriche generate nei giorni precedenti dall'app dell'utente.

«Una volta ricevute le TEK pubblicate dal sistema di backend, ciascun dispositivo su cui è installata l'app avvia il raffronto tra gli RPI ricavati dalle TEK scaricate e quelli, rilevati nei 14 giorni precedenti, memorizzati all'interno di ciascun dispositivo mobile, al fine di verificare la presenza di un contatto stretto con utenti accertati positivi al Covid-19» eseguendo, in pratica, un'operazione di matching tra i propri ID e quelli riferibili alle chiavi alfanumeriche scaricate.

Se l'app sullo smartphone di una persona trova una corrispondenza, a tale persona viene segnalato di essere stata in contatto con una qualcuno risultato positivo al Covid-19.



A questo punto, tuttavia, si evidenzia che il sistema predisposto non impone all'utente potenzialmente contagioso di compiere specifiche attività una volta ricevuta la notifica di esposizione.

Immuni, come chiarito nella sezione "domande" del sito e dell'app, offrirà dei suggerimenti che l'utente potrà seguire o meno (in ossequio al principio di volontarietà espresso nell'art. 6 D.L. 28/2020), come ad esempio "informare il proprio medico di base".

Ad entrare in gioco dovrebbe essere, quindi, il senso civico e la responsabilità dell'utente che pur non essendo certo – in assenza di sintomi e di test che lo confermino – di essere positivo al Covid-19 dovrebbe comunicare al proprio medico di base l'avvenuta notifica di Immuni e restare in autoisolamento, in ossequio a quel dovere di solidarietà di matrice costituzionale, e eventualmente, aspettare di effettuare i test.

Purtroppo, è proprio sotto questo punto di vista che il sistema mostra la propria forza dissuasiva rispetto alla possibilità dei cittadini di affidarsi all'uso di Immuni e il caso succitato della signora di Bari ne è l'emblema.

Molto importante sarebbe a questo punto della catena di tracciamento prevedere un sistema uniforme – quantomeno per regione – e standardizzato per procedere celermente

alla verifica di positività del soggetto che è stato esposto al rischio di contagio e lo abbia segnalato al proprio al sistema sanitario per il tramite del medico di base.

Conclusions.

Da quanto precede risulta con sufficiente chiarezza che il legislatore, il Governo e tutti gli attori che hanno preso parte alla realizzazione e che concorrono al funzionamento del sistema Immuni hanno profuso un grosso sforzo nel proporre una soluzione tecnologica privacy oriented che potesse avere una efficacia tangibile nella lotta alla diffusione del virus e che di fatto sembra rispondere alle esigenze di tutela e di scopo prefissate.

I rischi relativi all'uso improprio o distorto (anche in maniera involontaria) dei dati sono stati effettivamente ridotti al minimo, ma i dubbi sulla complessiva coerenza del sistema restano.

Considerata l'app Immuni in sé uno strumento che tiene al sicuro i dati e che tutto sommato opera in posizione di bilanciamento degli interessi in campo, il dato certo da considerare quale punto di partenza per riflettere sull'opportunità di usare l'app è la necessità[14], manifestata dalla comunità scientifica, di spezzare la catena dei contagi attraverso un sistema efficiente di tracciamento basato sulle tecnologie e che auspicabilmente si integri col sistema di assistenza offline dei soggetti potenzialmente contagiati ed accertati positivi, che ponga così rimedio ai limiti evidenti insiti nella mera ricostruzione "in via analogica" della rete di contatto di un soggetto risultato positivo.

I soggetti non consapevoli di essere stati esposti al virus e potenzialmente in grado di trasmetterlo ad altri in assenza di sintomi sono l'anello debole di quella catena che può essere spezzata proprio grazie all'ausilio di una app come Immuni ma, come detto, non esclusivamente grazie ad essa.

L'esperienza maturata ad oggi dimostra che questo strumento sconta il limite di una bassa diffusione dovuta, con tutta probabilità, in parte soprattutto al timore di esser sottoposti a misure limitative della libertà personale in maniera non giustificata.

"Analogico" e "digitale", dunque, come sostenuto anche in dottrina, sono due aspetti inscindibili del sistema costruito per la lotta contro il virus SARS-CoV-2. Sarebbe opportuno ripensarlo implementando la coordinazione tra i due mondi, facendo meglio comunicare ed interagire elemento umano e tecnologico, rendendo più rapido e certo il sistema di screening post notifica al fine di eliminare in tempi ragionevoli il dubbio sull'avvenuto contagio, nell'ottica di rendere davvero efficiente e meritevole di fiducia un sistema che richiede ai cittadini un sacrificio connesso alla compressione, seppure in maniera fortemente controllata, della privacy e, in alcuni casi, della libertà di movimento.

[14] In tal senso C. COLAPIETRO, A. IANNUZZI, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali,* in dirittifondamentali.it, 10 giugno 2020, fasc. n. 2., 772 - 803.

HAVE COLLABORATED TO THIS ISSUE OF THE *EJPLT*

ANTONIA ASTONE - Assistant Professor at Università degli Studi di Messina

LIVIA AULINO - Ph.D. (c) at Università degli Studi Suor Orsola Benincasa di Napoli, Member of the Editorial Team of EJPLT

SEBASTIÃO BARROS VALE - Lawyer in Portugal, LL.M in EU law at the College of Europe

DMITRY E. BOGDANOV – Professor of Private Law at Kutafin Moscow State Law University

VIOLA CAPPELLI - Ph.D. (c) in Law at Scuola Superiore Sant'Anna di Pisa

ANNA IRENE CESARANO - Ph.D. (c) at Università degli Studi Suor Orsola Benincasa

NICOLETA CHERCIU – Research Fellow on the Regulation of Robotics and AI AT Scuola Superiore Sant'Anna di Pisa, Lawyer

TEODOR CHIRVASE – Legal Counsel, LL.M. in Law & Technology at Tilburg University

MASSIMO CICORIA - Ph.D. at Università degli Studi di Napoli Federico II, Lawyer

ANTONELLA CORRENTI –Research Fellow in Private Comparative Law at Università degli Studi di Messina, Lawyer

ANDREA D'ALESSIO - Ph.D. at Università degli Studi di Teramo, Lawyer

LEONARDO ESPINDOLA - Industrial Designer at Humatects GmbH

MIRKO FORTI - Research Fellow at Scuola Superiore Sant'Anna di Pisa

MARIA CRISTINA GAETA – Postdoctoral Research Fellow in Private Law at Università degli Studi Suor Orsola Benincasa, Coordinator of the Editorial Team of EJPLT, Lawyer.

PAOLA GRIMALDI - Ph.D. at University of Naples Federico II, Lawyer

SERGIO GUIDA - Independent Researcher, Data Governance & Privacy Sr Mgr

MARIE-CHRISTIN HARRE - HMI Engineer at Humatects GmbH

ALDO IANNOTTI DELLA VALLE - Ph.D. (c) at Università degli Studi Suor Orsola Benincasa, Lawyer

ARNDT KÜNNECKE - Federal University of Applied Sciences for Public Administration Brühl

SIMONA LATTE - Legal Counsel e Web Marketing Manager

VALERIA MANZO - Ph.D. (c) at Università della Campania Luigi Vanvitelli, Member of the Editorial Team of EJPLT, Lawyer

SILVIA MARTINELLI - Postdoctoral Research Fellow at University of Milan, Lawyer

ANNA ANITA MOLLO –Ph.D. at Università degli Studi Suor Orsola Benincasa, Lawyer

ROBERTA MONTINARO - Associate Professor of Private law at Università degli Studi di Napoli L'Orientale

FABRIZIA ROSA - Ph.D. (c) at Università degli Studi di Napoli Parthenope

MARCEL SAAGER - M.Sc., Modelling & Software Engineer at Humatects GmbH

CHIARA SARTORIS - Postdoctoral Researcher in Private Law at Università degli Studi di Firenze

PASQUALE STANZIONE - President of the Italian Data Protection Authority

LAURA VALLE – Associate Professor of Private Law at the Free University of Bolzano