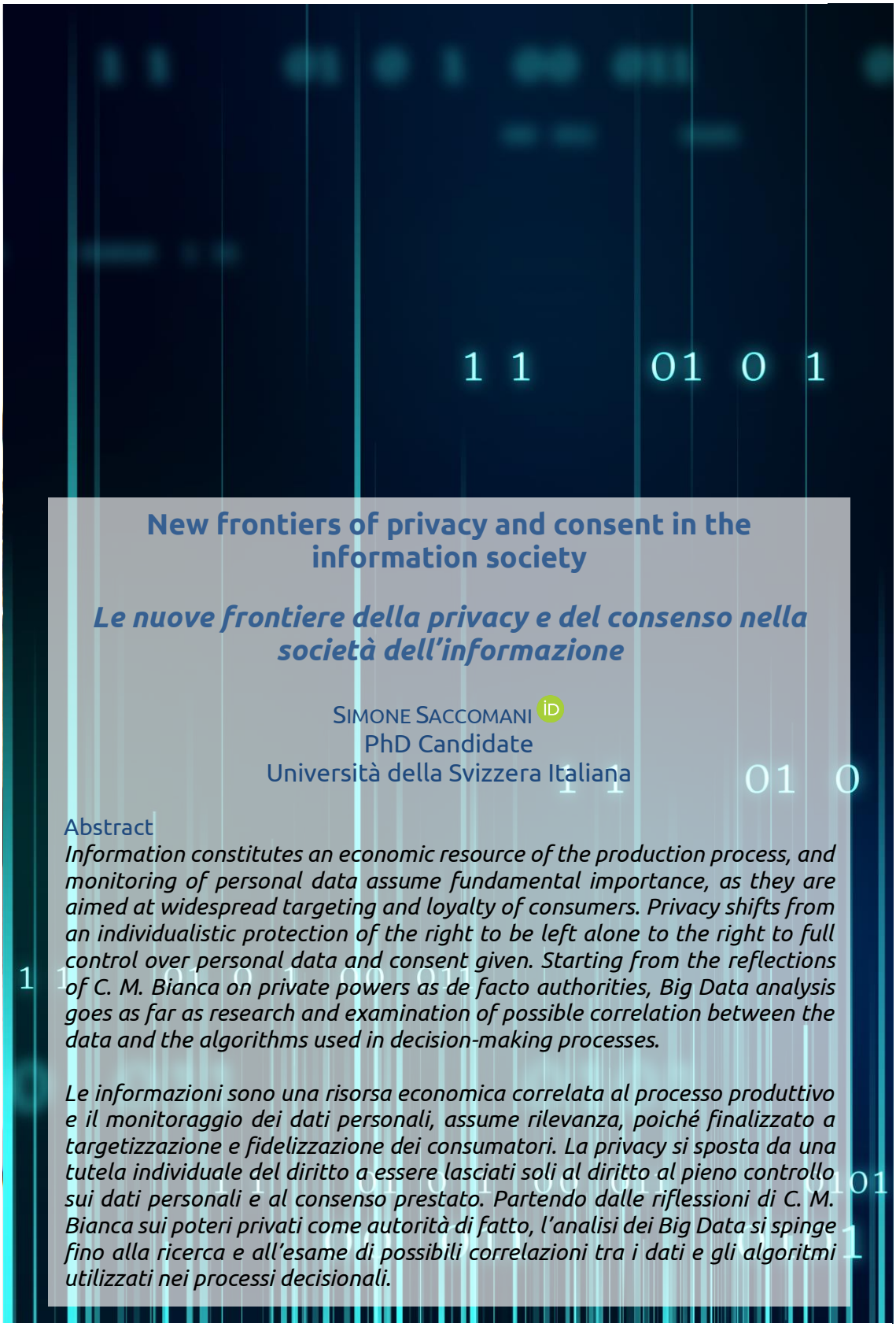
Saccomani S, 'New frontiers of privacy, and consent in the information society ' (2024) 2 EJPLT.
DOI:

EJPLT
ISSN 2704-8012



New frontiers of privacy and consent in the information society

Le nuove frontiere della privacy e del consenso nella società dell'informazione

SIMONE SACCOMANI
PhD Candidate
Università della Svizzera Italiana

Abstract

Information constitutes an economic resource of the production process, and monitoring of personal data assume fundamental importance, as they are aimed at widespread targeting and loyalty of consumers. Privacy shifts from an individualistic protection of the right to be left alone to the right to full control over personal data and consent given. Starting from the reflections of C. M. Bianca on private powers as de facto authorities, Big Data analysis goes as far as research and examination of possible correlation between the data and the algorithms used in decision-making processes.

Le informazioni sono una risorsa economica correlata al processo produttivo e il monitoraggio dei dati personali, assume rilevanza, poiché finalizzato a targetizzazione e fidelizzazione dei consumatori. La privacy si sposta da una tutela individuale del diritto a essere lasciati soli al diritto al pieno controllo sui dati personali e al consenso prestato. Partendo dalle riflessioni di C. M. Bianca sui poteri privati come autorità di fatto, l'analisi dei Big Data si spinge fino alla ricerca e all'esame di possibili correlazioni tra i dati e gli algoritmi utilizzati nei processi decisionali.

* Il presente contributo è destinato allo special issue in memoria del Prof. Cesare Massimo Bianca e del Commentario al D. Lgs. 30 giugno 2003, n. 196 «Codice della privacy» da lui curato con il Prof. Francesco Donato Busnelli nel 2007 (Cedam).

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Information, consent, personal data, big data, algorithms.

Summary: Introduction. – 1. Consent to privacy in the context of the information society. – 2. Big Data in the Information Society. – 3. Big Data, smart cities and consent to the processing of personal information. – 4. Conscience and freedom in giving consent. – Conclusions.

Introduction.

In the current context, platforms have assumed a decisive role, so much so that they have become real private powers.[1] Taking up Cesare Massimo Bianca's distinction, it is possible to qualify private powers as de facto authorities.[2]

At the beginning of the 1990s, Norberto Bobbio wrote in his book "L'età dei diritti": "We have entered the era that is called postmodern, characterized by the enormous, dizzying, and irreversible advance of technological transformation, and consequently also of the technocratic world. From the day Bacon said that science is power, man has come a long way!"[3]

Bobbio understood that the defined rights of the new generation arise, fundamentally, from technological development and the possible effects of the latter on the right to life, liberty, and personal security.[4]

In fact, in no case can one conceive of an indifference to the traditional framework of rights in the current context, characterized by the unstoppable advance of information technologies, which makes the traditional contrast between old and new rights irrelevant, thus highlighting the full capacity of the law to adapt to the changes of a complex and moving society.[5]

In this article, starting from the reflections of C. Massimo Bianca[6] on data protection and responsibility[7], focusing on the effectiveness of consent with special attention to Big Data, it will be observed that the possibility of collecting, processing and cross-referencing personal information has led to a redefinition of the private sphere, particularly of individual self-determination and the provision of a consensus capable of placing knowledge and the effectiveness of its guarantee at the center of attention and reflection.[8]

A positive law method is applied for the analysis of the issues discussed in this paper. After an examination of the state of the art and an in-depth study inherent in the Euro-Union privacy law and how increasingly pervasive smart devices have changed the human-machine relationship. It is also analyzed, also

[1] P Stanzone, *I "poteri privati" delle piattaforme e le nuove frontiere della privacy* (Giappichelli, 2022) 1-3.
[2] C M Bianca, *Le autorità private* (Jovane, 1977) 2-5; M Grondona, 'Poteri dei privati, fonti e trasformazioni del diritto: alla ricerca di un nuovo ordine concettuale' in P Serena A Zoppini (eds.), *I poteri privati e il diritto di regolazione* (Roma Tre Press 2018) 5-28.
[3] N Bobbio, *L'età dei diritti* (Giappichelli 1990) 253.
[4] S Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli* (Laterza 2012) 31-69.
[5] C Faralli, 'Introduzione', in A Ballarini (ed.), *Novecento del diritto* (Giappichelli 2019) 1-8.
[6] S Patti, 'Consenso, sub art. 23)', in *La protezione dei dati personali. Commentario* C M Bianca, F D Busnelli (eds.), t. I (Cedam 2007) 541 ff.
[7] E Del Prato, 'Riflessioni conclusive', in M Bianca (ed.), *La responsabilità. Principi e finzioni. Continuando a dialogare con Cesare Massimo Bianca* (Wolters Kluwer 2023) 380-387.
[8] A Caligiuri, *Legal Technology Transformation* (Editoriale Scientifica 2020) 1.

considering Cesare Massimo Bianca's reflections, how in consensus and its discipline over time have changed. At the empirical level, some practical cases are examined for an actualization and concretization of theoretical reflections.

1. Consent to privacy in the context of the information society.

Information in the so-called new economy, constitutes one of the main economic resources of the production process and capacity.[9] New technologies are imposing new languages and new tools in contemporary society.[10]

Controlling and selling knowledge represents a sophisticated and profitable form of commercial exchange, where the greatest benefit comes not so much from traditional production processes and products, but from the control of information and market trends that allow optimizing the relationship between supplier and user, in the direction of customer loyalty.[11]

Therefore, the collection, meaningful selection of information and its monitoring, aimed at an increasingly wide audience, capable of identifying and profiling the characteristics of the individual consumer, seems to be of fundamental importance. [12] The delimitation of individual profiles and preferences, in turn, contributes to influencing subjective behaviors, as demonstrated, in a very significant way, by the phenomena of early shipment and sale, developed by Amazon, capable of anticipating and inducing, apparently without any force, future purchases by customers.[13]

Marco Delmastro and Antonio Nicita argue that "the effectiveness of the digital revolution is also manifested in the 'recommendations', in the algorithmic 'suggestions' that we receive from search engine ads or featured on e-commerce sites: opportunities that could be of interest, as they have interested others, similar to us, before us"[14]

The traditional debate on privacy, which shifts from protecting individual confidentiality to increasingly emphasizing the guarantee and control of one's own information, intensifies when it involves the monetization of data. This occurs when privacy itself becomes an economic resource, and users trade it for free services.[15] It is evident that personal information is intimately linked to the rights of the person and thus raises pressing ethical and legal issues for

---

[9] A Maceratini, 'New Technologies, Big Data and Human Righ.ts: An Overwiew', in A Caligiuri (ed.), *Legal Technology Transformation* (Editoriale Scientifica 2020)11-20.

[10] it emerged that the usability of Microsoft's Windows 10 operating system is medium-low. In particular, the examination of biometric data shows that even those who declare that the protection of privacy matters then opts for the default data settings. The reason is that obviously the user is not perceiving the risk. Microsoft also exploits cookies for various purposes, including storage of preferences and settings; access and authentication; safety; storage of information provided by the user to a website; social media; feedback; interest-based advertising; display of advertisements; analysis; performance. R Moro Visconti, 'Evaluation of the Big Data and Impact on Innovation and Digital Branding', (2016) 1 Industrial Law, 46,51.

[11] J Rifkin, *The Age of Access: The new Culture of Hypercapitalism, Where All of Life is a Paid-for-Experience* (Penguin 2000) 65.

[12] L Gatt, R Montanari, and I A Caggiano, 'Consent to the Processing of Personal Data: A Legal and Behavioural Analysis. Insights into the Effectiveness of Data Protection Law.' (2018), 1 *EJPLT* 1,15.

[13] D Talia*, La società calcolabile e i big data. Algoritmi e persone nel mondo digitale*, (Rubettino, 2018) 25-40.

[14] M Delmastro A Nicita, *Big data. Come stanno cambiando il nostro mondo* (EDB 2019)13.

[15] 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' (2017) 2 Politica del diritto 343,360.

its economic exploitation, which implies the protection of fundamental rights.[16]

The concept of privacy, in the double sense of guaranteeing the most private sphere of the human being and protection of the personal data that affects him, has undergone considerable evolutions over time and space.[17]

Here we can only briefly mention this path, and it is worth remembering that already in the remotest antiquity man sought moments of solitude to protect his private life and had developed the concept of confidentiality and secrecy of information.[18]

The modern origins of the concept of privacy can be traced, in any case, to two American jurists, Samuel Warren and Louis Brandeis who, in the 1890-91 volume of *the Harvard Law Review*, published the essay *The Right to Privacy*.[19]

In this work, which arose from the controversy against the *Evening Gazette* newspaper, accused by Warren of undue interference in his wife's private life, the two authors ask precisely which information about private life should remain secret and which, otherwise, could become news of public knowledge and domain, thus outlining the right to privacy through the intrinsic value it has for its owner.[20]

The notion of privacy and related consent was later expanded to the point of currently talking about computer privacy, to indicate the need to have control over the flow of personal information that circulates through electronic computers and the telematics network, data that, if interpreted correctly, is capable of revealing the most secret details of human existence.[21]

In Italy, the rules relating to the protection of personal data are contained in the "Code on the Protection of Personal Data" (Privacy Code), a provision intended to bring together the innumerable provisions of the sector that have been produced over the years and to introduce the most significant innovations of the Guarantor Authority and the European Directives on the confidentiality of electronic communications.[22]

Among the latter, it is necessary to mention the EU Directive n.95/46, on the protection of natural persons with regard to the granting of consent to the processing of personal data, with the aim of harmonizing the rules on the protection of personal data, of ensuring a free flow of data and promoting a high level of protection of the fundamental rights of European citizens, including that inherent to the provision of privacy consent. This provision was recently repealed by the General Data Protection Regulation (GDPR: EU Regulation No. 2016/679) aimed at strengthening the confidentiality of private information by implementing the system of responsibilities and security

---

[16] S Palanza, 'Internet of things, big data e privacy: la triade del futuro', (2016) 16 *IAI, Documenti Istituto Affari Internazionali*, 1,7, is available here: <https://www.iai.it/sites/default/files/iai1612.pdf> accessed 29 July 2024.

[17] A Ballarini, *Novecento del diritto* (Giappichelli 2019) 1 ff.

[18] F A Schreiber, L Tanca L, *Etica e big data, sette principi per proteggere i diritti umani*, is available here:<https://www.agendadigitale.eu/cultura-digitale/etica-e-big-data-sette-principi-per-proteggere-i-diritti-umani-fondamentali/> accessed 29 July 2024.

[19] S D Warren, L D Brandeis, *The Right to Privacy* (Quid Pro 2015) 1-98.

[20] G De Minico, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria* (2019) 89 (1) *Diritto pubblico* 109,113.

[21] G Pascuzzi, *Il diritto dell'era digitale* (Il Mulino 2016)48.

[22] Maceratini, 'New Technologies, Big Data and Human Righ.ts: An Overwiew' (n.9) 11-20.

measures to protect information.[23]

The current meaning of privacy, from the individualistic and essentially passive protection of the right to be left alone to the right to total control of the information that concerns us, is also sanctioned by the Charter of Fundamental Rights of the European Union (Charter of Nice of 2000, which in its art. 8 provides for the right to the protection of personal data), as well as by the Declaration of Internet Rights of our country, made public on October 13, 2015, on an international conference held in the *Sala della Regina* of the Montecitorio Palace.[24] This text is essential to guarantee everyone the exercise of active digital citizenship, in full respect and appreciation of the freedom, dignity and diversity of each person, fundamental elements of a society of dignity, equality, freedom and participation.[25]

2. Big Data in the Information Society.

Bianca argues that the Art 810 c.c. constitutes a rule of foundational value in the Italian legal system and in continental legal systems in general; the distinction between what is a good[26] i.e., an object of law, and what is not.[27]

Central to the information society is the idea of sharing data, which can be found wherever there is a memory device for data: these, if analyzed individually, may not be particularly significant, but, if information technologies are examined with appropriate attention and in large volumes, they can lead to the delineation of patterns and trends. capable of producing knowledge adequately.[28]

In this sense, it is evident how the omnipresence of information technologies, mainly, as we will see later, the *Internet of Things*[29], has increased and facilitated digital surveillance practices, making anyone who uses a networked computer device easily traceable and monitorable.[30]

A possible solution, proposed to overcome the problem, has been identified in the limitation of the maximum number of variables to be used in *Big Data* analysis, but, even in this hypothesis, the problem of data extracted unexpectedly would remain open, as well as more information obtained thanks to the predictive effectiveness of the algorithms used.[31]

This phenomenon is aggravated by the fact that, frequently, the user signs a

---

[23] D.L 10.08.2018, n.101

[24] S Rodotà *Discorso conclusivo della Ventiseiesima Conferenza Internazionale sulla protezione dei dati* (Breslavia, 13-16 September 2004) is available here< https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293> accessed 29 July 2024.

[25] S Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, (Laterza 2012)31-69.

[26] CM Bianca, 'La proprietà', in Id. *Diritto civile*, 6, (Giuffrè 1999) 49-54.

[27] L Gatt, 'Legal anthropocentrism between nature and technology: the new vulnerability of human beings' (2022) 1 EJPLT 15,26.

[28] Talia, 'La società calcolabile e i big data. Algoritmi e persone nel mondo digitale', (n.12) 39-40.

[29] The Internet of Things (hereinafter "IoT"), an expression coined by British researcher Kevin Ashton in 1999, expresses the transition from a network of interconnected computers to a network of connected everyday objects, facilitated by the development of wireless and satellite technology. On the IOT, preliminarily, P Paganini, 'Verso l'Internet delle cose', (2015) 1 Dir. Ind., 107 ff.

[30] Palanza, 'Internet of things, big data e privacy: la triade del futuro', (n.15) 2.

[31] F. Casi, *Big Data ed etica dei dati*, 2018, pp.1-3, is available here: <https://www.consultadibioetica.org/big-data-ed-etica-dei-dati-di-fiorello-casi/> accessed 26 July 2024.

single contract with the same provider of services such as Internet, telephone, and television, transferring large amounts of information into the hands of a single subject.[32]

From these suggestions, it is easy to understand how the term personal data should currently be understood in evolutionary terms, that is, following the direction indicated in the 2013 OECD Guidelines [33] , and considering as information all personal information that, together with other data of the same individual, may have effects on the same individual. Likewise, the concept of privacy should be extended to information that, although it is outside the scope of subjective lordship, helps to identify it.[34]

As Marzia Orefice states, strictly speaking, "not even on the data that is published on the Internet for a specific purpose does the user intend to renounce the expectation of privacy".[35]

In the analysis of personal data, it can be observed how, paradoxically, the predictions seem much more exhaustive and significant than the information disclosed through explicit and informed consent on the part of users. This also happens in political communication and an example was the Italian 2020 Constitutional Referendum [36]

In other words, "big data analytics models make it possible to reconstruct personal data, regardless of its original disclosure, making the traditional classification between personal data and non-personal data completely obsolete."[37]

Consequently, a proper consideration of technological evolution seems to lead to a broad and changing interpretation of the concept of personal data, also including the information produced by "smart" objects.[38]

According to the OECD definition, Big Data is any user-generated content on the Internet, including blogs, photographs, videos, behavioral data, social data,

---

[32] Z Bauman, *Consuming Life* (Polity Press 2007) 1 ff.

[33] OECD *Guidelines governing the protection of privacy and transborder flows of personal data.* Is available here: <https://www.oecd.org/en/topics/digital.html> accessed 24 July 2024.

[34] M Orefice, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, (Aracne 2018) 100-104.

[35] Ivi, p. 105.

[36] For example, on the 2020 Italian constitutional referendum, the communication on Facebook of those opposed to the referendum question certainly focused on an anti-populist dimension and on a rhetoric focused on new narratives with respect to the themes of the referendum campaign. In fact, making a comparison with what had been envisaged in the definition phase of the research hypotheses, the communication products that generated the greatest engagement were characterized by an interactional type of communication and an active style, but by communication formats suited to the logic of social media, such as videos, and by new themes, little explored in the debate during the electoral campaign, among which the reference to the themes of the media presence of the various referendum fronts stands out, which in this referendum campaign actually seemed a theme worthy of attention during and after the electoral period. The poor success, in terms of engagement, of contents that refer to typical themes of anti-populist political discourse, such as the representativeness of the elites and the representativeness of the territories, which seemed to be able to become central also in light of the specific referendum theme, and the lack of success of contents characterized by an antagonistic vision seems therefore to be explained by a greater value attributed by Facebook users to a rhetorical communication style based on elements initially typical of populist communication, and recently adopted by right-wing populism, such as the battle against the media. P Ferrucci, T Hopp, C J Vargo, C. J., 'Civic engagement, social capital, and ideological extremity: Exploring online political engagement and political expression on Facebook', 22 (2020) 6 New media & Society, 1095,1115.

[37] Delmastro Nicita, 'Big data. Come stanno cambiando il nostro mondo ', (n.13) 36.

[38] M C Gaeta, 'Data protection and self-driving cars: the consent to the processing of personal data in compliance with GDPR' (2019) 24 (1) Communications Law,1,9.; M C Gaeta, 'La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi' (2018) 1 Diritto inf. e informatica, 147,179.

geolocation data, demographic data, and identification data in general: content that allows individual identification or provides information about typical patterns of individual behaviors.[39]

It should be noted that art. 1 of the proposed Regulation on Privacy in Electronic Communications (Privacy Regulation) does not include in the category of metadata all data other than content, however, only those processed on the network and not also data processed on devices, as also pointed out in the European Championship Guarantor Privacy Opinion of 6/2017.[40]

Big Data can also be described using the so-called "4Vs": volume, as they exist in large quantities; variety, due to their diverse sources; velocity, as the data is processed by sophisticated algorithms that enable real-time decision-making; and value, which the data inherently possesses.[41]

It should be noted that most of this data is usually unstructured, as it is acquired and stored according to criteria different from those that govern the organization of traditional electronic files.[42]

the peculiarity and potential of Big Data, capable of causing a real paradigm shift in the analysis of information, lies in the fact that it has not been extrapolated from representative samples of the population through complex and expensive processes, but directly from the entire population observed, so that, in terms of predictive effectiveness, by exploiting all possible correlations, their quantity prevails over the precision of the analysis procedure.[43]

In the use of Big Data, the aspiration and the need for precision are weakened. In fact, the presence of fewer errors, necessarily, in the sampling, allows us to accept some inaccuracies in the calculation.[44]

This allows us to go beyond traditional methods of data analysis, based on the search for causal relationships, to examine all possible correlations.[45]

Fiorello Casi argues that with Big Data it is only possible to investigate and discover, identify, and analyze trends and correlations. Significant in this regard is the case of the Facebook platform called CrowdTangle which proposes an in-depth analysis of the epistemological problems and methodological implications of its use in the investigation of social phenomena in digital spaces [46] In many activities it is not always necessary to know the cause of a

[39] Palanza, 'Internet of things, big data e privacy: la triade del futuro', (n.15) 16.
[40] Delmastro Nicita, 'Big data. Come stanno cambiando il nostro mondo ', (n. 13) 35.
[41] A C Amato Mangiameli, 'Algoritmi e big data. Dalla carta sulla robotica' VIII (2019),1 Rivista di filosofia del diritto, 107,124.
[42] S Simoncini, S Suweis, 'Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale' VIII (2019), 1Rivista di filosofia del diritto87, 106 Delmastro Nicita, 'Big data. Come stanno cambiando il nostro mondo ', (n.13) 10.
[43] Amato Mangiameli, 'Algoritmi e big data. Dalla carta sulla robotica', (n.39) 112.
[44] Casi, 'Big Data ed etica dei dati' (n.30) 1-3.
[45] G Della Morte, *Big Data e protezione internazionale dei diritti umani. Regole e conflitti* (Editoriale Scientifica 2019) 161 ff.
[46] CrowdTangle presents itself as a tool whose pitfalls lie in several points. First, it provides aggregated data and does not allow researchers to explore comments and responses associated with posts on public pages and groups. Furthermore, the same preset variables refer to the dimension of engagement, betraying an epistemology of online platforms based on the logic of selling contacts to advertisers. If in the first case, further manual analyses allow for the construction of ad hoc variables and the carrying out of more refined analyses guided by one's own research hypotheses, in the second case even the same criticism of the algorithm for calculating the engagement rate can be overcome by reconstructing a new engagement variable in a manner guided by one's own research interests. The development of analyses that also refer to

phenomenon, but it is more than enough to identify how it acts and interacts with others and what correlations are established between them.[47]

This describes an exploratory analysis based on inferences, in which the machine "learns directly" from the data and where the process of processing and aggregating the information is relevant with the algorithms used in the process, aimed at reaching a "decision".[48]

In this way, Big Data implements the use of the algorithm while, in turn, the use of the algorithm generates new data, and so on. It should also be noted that Big Data analysis is usually accompanied by the examination of Small Data, i.e. information not generated by data correlation, but detected by observing the user's behavior and routines, inserted in the usual context of action. According to Martin Lindstrom, the observation of people's behavior, of their daily and routine actions in their natural environment, rather than in a database, may be more important in terms of subjective decision-making processes.[49]

Equally significant seems to be the study of metadata, that is, information that is associated with a web page, or a part of it, that represents the content and the reference context in a structured way.[50]

Data, therefore, as a description of potentially reproducible facts, becomes real information when it is extracted, processed, and used for specific purposes. In this sense, we can well understand how the correct use of Big Data represents a critical factor for companies, in the constant improvement and personalization of the services offered to users: huge amounts of data, if not interpreted and used effectively, run the risk of being equally ineffective due to the scarcity of information.[51]

Sudden economic and social developments require the agility of the media and, in this context, adequately exploiting the potential wealth of all information constitutes an undoubted competitive advantage and represents a factor that generally motivates widespread business opposition to certain policies on data portability.[52]

To transform data into meaningful information, computer techniques are used, such as Data Mining, the process of extracting knowledge from large databases, through the application of algorithms that identify and explain the associations between data.[53]

---

multivariate statistical techniques during the research work has also implied the need to connect digital research and critical data analysis, also in a statistical sense: as highlighted by Tromble, looking critically at what the data represents, being more open about the treatment of the data and developing better approaches to draw inferences with a broader value means in fact questioning the meaning of the data from both a contextual and statistical point of view. R Tromble, 'In Search of Meaning: Why We Still Don't Know What Digital Data Represent', 1 (2019) 1Journal of Digital Social Research, 17,24; G Punziano, F Marrazzo, S Acampa (2023) 'La campagna per il Referendum Costituzionale 2020 e la comunicazione antipopulista su Facebook: un'applicazione di Content Analysis dagli esordi accademici del primo Crowdtangle', 13 (2023), 25 Cambio. Rivista sulle trasformazioni sociali», 249, 226.

[47] Casi, 'Big Data ed etica dei dati' (n.30) 3.

[48] Simoncini, Suweis, 'Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale', (n.40) 92.

[49] M Lindstrom, *Small Data: i piccoli indizi che svelano grandi trend* (Hoepli, 2016)15-36.

[50] Palanza, 'Internet of things, big data e privacy: la triade del futuro', (n.15) 7.

[51] Orefice, 'I Big Data e gli effetti su privacy, trasparenza e iniziativa economica', (n.33) 62.

[52] Amato Mangiameli, 'Algoritmi e big data. Dalla carta sulla robotica', (n.39) 108.

[53] G De Anna, 'Automi, responsabilità e diritto', VIII (2019), 1 *Rivista di filosofia del diritto* 125, 142.

Data Mining represents a process within which one or more techniques are used to extract knowledge from large amounts of data, in terms of associations, patterns, rules or repeated sequences, subsequently allowing personal data to be cross-referenced to extract trends and convergences that help, in the first place, the marketing sector in the loyalty of its customers. This cognitive process is currently continued by Business Analytics and is summarized here as the set of tools and software applications for data access, analysis, and visualization that help management quickly capture relevant information and monitor the company's performance in making more effective decisions. Through these procedures of research and extraction of useful information from large amounts of data, using automatic or semi-automatic methods and their mainly corporate and industrial use, individuals are progressively assimilated to the sensors of the environment, a condition accentuated by the progressive appearance of the Internet of Things.[54]

The Internet of Things (IoT) expresses the transition from a network of interconnected computers to a network of connected everyday objects, facilitated by the development of wireless and satellite technology that enables the effective management of an increasing amount of information.[55]

We are faced with the phenomenon of intelligent everyday objects, that is, capable of interacting with each other and with users, developing the inherent potential of the Internet towards innovative applications of information from the environment.[56]

The latest advancements on the Internet of Things mark a new evolution determined by the attempt to connect all existing objects: this is why we speak of the Internet of Everything (IoE), a phenomenon that futuristically, but not so much, would see people, data and procedures using systems capable not only of memorizing, but also of learning and generating information.[57]

3. Big Data, smart cities, and consent to the processing of personal information.

The cooperative and participatory use of some types of Big Data in the public sphere has a certain social interest. As Silvio Bolognini states, the 'smart city' paradigm currently represents a vision of the city that is widely shared on a global scale.[58]

A multidimensional representation of the urban context focused on the technological element, an enabling factor for an innovative and polarised development of the urban system: from energy consumption to mobility, from public administration management to security, from employment policies to

[54] C Sarra, 'Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining', in P Moro, C Sarra (eds), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, (FrancoAngeli 2017), 41-63.
[55] M Iasselli 'Privacy e nuove tecnologie', in M. Iasselli(ed.), *Diritto e nuove tecnologie. Prontuario giuridico ed informatico*, (Altalex 2016), 121-194.
[56] M Calvo, F Ciotti, G Roncaglia, M A Zela, *Internet 2004. Manuale per l'uso della Rete*, (Laterza 2003),585-586.
[57] R H Weber, 'Internet of Things. New security and privacy challenges' (2010) 26 (1) Computer law & security report 23, 30; E Welbourne, L Battle, G Col and others, 'Building the Internet of Things Using RFID: The RFID Ecosystem Experience' (2009) 13 (3) Internet Computing IEEE 48, 55.
[58] S Bolognini, *Dalla "smart city" alla "human smart city" e oltre* (Giuffrè 2017) 1-4

services to the person.[59] The representation of the city in a smart key also underlies a specific model of economic and social development, strongly contextualized in the competitive scenario of the global market, which redesigns the relations between the public and the private in the planning, programming and implementation of urban policies, with significant implications, at least in the theorizations of the concept of "smart city"", on the role of the citizen, hence the creation of the terms "smart citizen" and "smart citizen".[60]

At the epistemological level, by virtue of its focus on the technological factor, the emerging paradigm has paved the way for a public knowledge approach characterized by high claims of preparatory for an equally scientific legitimization of political options as options based on the detection, measurement, and analysis of data massively generated by the sensory and digital infrastructure of the urban fabric.[61]

Hence the proliferation of city rankings and benchmarks used as tools for a new politically neutral decision-making, which takes away from the debate between alternative visions of urban development.[62]

This is the case of the exchange of information on urban traffic, aimed at obtaining the essential knowledge that allows a city to be transformed into a smart city, as well as the case of the monitoring of data on traffic and pollution, aimed at implementing the protection of the territory and the environment, but, above all, the scientific context is one in which Big Data and its sharing acquire decisive importance, since sharing scientific research and its results seems fundamental.

Big Data, as Floriano Casi recalls, is taking the world stage as one of the most powerful and fascinating disciplines of all time, mainly because of the opportunities it offers in all fields, from politics to economics, in social research, in culture and in all scientific research.[63]

The collection and monitoring of big data in these areas acquire great importance, as the information gathered supports the exchange of knowledge and equality. This serves as a foundation for democratic participation, as highlighted in Article 19 of the Universal Declaration of Human Rights and Article 21 of the Italian Constitution, which guarantee free and legally protected access to knowledge and culture.[64]

In addition to the economic and social advantages, it is worth highlighting some of the main critical issues that arise from the use of Big Data, which refer, first of all, to the protection of personal data and consent to the processing of these.[65]

---

[59] 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 (6) Computer Law & Security Rev. 643,660.
[60] S Bolognini, *Epistemologia e politica del diritto nella prospettiva delle "smart cities"* (Giuffrè 2016) 1-15.
[61] Bolognini, 'Dalla "smart city" alla "human smart city" e oltre', (n.55) 2.
[62] R De Santis, A Fasano, N Mignolli, N Vill, *Smart cities: theoretical framework and measurement experiences*, in *Italian National Institute of Statistics Istat*, 20 September 2013, 50 MPRA 207, 210.
[63] Casi, 'Big Data ed etica dei dati' (n.30) 3.
[64] L Nosari, *Potenzialità e problematiche afferenti all'utilizzo dei Big Data in materia di diritti umani*, in: Potenzialità e problematiche afferenti l'utilizzo dei Big Data in materia di diritti umani – CyberLaws
[65] J Drexl, 'Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of post-truth politics', (2016) 16 *Max Plank Institute for Innovation and Competition Research*, 1-28.

As far as the economic exploitation of personal data is concerned, it is necessary to verify whether the granting of consent for the use of personal data, which often occurs on the part of the data subject in a completely automatic manner, if not completely unconscious, is or is not present to a joint transfer of ownership rights over the personal data or whether the expression of consent does not rather represent a delegation to the exclusive use of the personal data. data, functional to identify the owner of the information and allow the provision of the service.[66]

In fact, there is a certain difference between the awareness of expressing 'formal' consent to use your data and that of participating in a real economic transaction on your data.[67]

This ambiguity raises urgent questions about the effectiveness of digital privacy protection, as well as about the due respect for competition between operators in the sector, a factor that significantly affects the regulation of markets.[68]

In the case where one leans towards the hypothesis of the transfer of an exclusive delegation, it can be observed, in fact, that the latter, if on the one hand avoids the indiscriminate transfer of personal information, avoiding a possible data market, while allowing a monopolistic use of information on the online platform.[69]

In this sense, the public good (information) becomes de facto a private property, but only for the platform that uses it. The joint use of multiple online platforms by users (multihoming) could partly and under certain conditions mitigate this phenomenon.[70]

Based on these considerations, as C M Bianca argues[71], this could be the way forward to overcome the principle of exclusive delegation in favour of the transfer of a property right relating only to some uses of personal data, ensuring that certain information remains limited to the most confidential sphere, while others remain publicly shared.[72] In this sense, the recognition of the right to the portability of personal data, enshrined in art. 20 of the GDPR, seems to correspond to this logic, which will also apply to unstructured data that would not require any manifestation of consent since its extraction occurs outside of a specific transaction. It should be noted that the transfer of data and its economic valorisation are not only relevant in reference to the protection of privacy, but also for the purposes of the legal, as well as economic, construction of a transparent data market and, in this regard, it should be remembered that the GDPR has significantly reinforced the obligations of transparency in the processes of acquisition and processing of personal data.[73]

---

[66] Delmastro Nicita, 'Big data. Come stanno cambiando il nostro mondo ', (n.13) 30.
[67] Ibid., 42-43.
[68] M C De Vivo, *Comunicare in Internet. Con che diritto?* IX (2020), 2 *Informatica e Diritto*, 125,158.
[69] Ibid., 156-158.
[70] Delmastro Nicita, 'Big data. Come stanno cambiando il nostro mondo ', (n. 13) 127.
[71] C M Bianca, 'Note introduttive' in C M Bianca, F D Busnelli F.D. (eds) *La protezione dei dati personali. Commentario, vol. I* (Cedam 2007), XIX-XXIV.
[72] I.A. Caggiano, 'A quest for efficacy in data protection: a legal and behavioural analysis' (2017) 10 WP 2,18.
[73] L Gatt, I A Caggiano R Montanaro, *Privacy and Consent. A Legal and UX&HMI Approach for Data Protection*, (Suor Orsola Benincasa University Press, 2021) 83-100.

4. Conscience and freedom in giving consent.

Another complex and relevant problem refers, then, to the difficulty of determining when and to what extent the user is aware of the collection of personal data and its processing, considering that access to specific data is not always an indispensable condition for the use of a service.[74]

Computer mechanisms, such as tracking walls, can exclude users from a given service who refuse to extend consent to another service, or act as factors of marginalization and forcing consent, as is also the case with device tracking.[75]

In these hypotheses, the apparently free acceptance of users allows companies to exploit personal information, raising serious questions about the protection of privacy and freedom of expression, since, to hide the individual, they could, as a last resort, give up the freedom to choose the content to access and the sites to visit on the network.[76]

In this scenario, refusing to provide personal information would result in exclusion from an increasing number of social activities, from access to information to receiving goods and services.[77]

These practices, although widespread, are in conflict with Art. 4 of the GDPR on informed consent, since, in fact, a request that meets non-homogeneous purposes or that prevents or disrupts the use of a service offered online does not comply with the Regulation – as well as with the requirement of freedom of consent, since it does not, it can be said that it is effectively free of charge when its assignment constitutes the price of the service.[78]

As Margaret Vestager, European Commissioner for Competition, emphasized in October 2014, data is the new currency of the Internet and therefore cannot be considered free, a term that implies self-determination and freedom, even though online services are provided in exchange for personal data. Doubts about the freedom to grant consent are further intensified if we consider the current indispensability of some services in interpersonal communications. In this sense, as Stefano Rodotà argues, what seems to us a banal tool to obtain free access is the real good, the exchange of which underpins the underlying commercial transaction. The implicit exchange, for all these free services, is with our attention, with the release of data that will then allow promotions and advertising personalized to our needs. This implicit exchange corresponds to an implicit market, that of data, about which we still know very little. As is often repeated in these cases, the product is us.[79]

It should be noted that the European Regulation does not directly mention Big Data, inexplicably excluding data collected and cross-referenced daily, capable of providing sometimes more than sensitive information about the individual and capable of profoundly impacting the development of

[74] Amato Mangiameli, 'Algoritmi e big data. Dalla carta sulla robotica', (n.39) 112.
[75] A C Zanuzzi, 'Internet of things e privacy. Sicurezza e autodeterminazione informativa', in P Moro, C Sarra (ed.), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, (FrancoAngeli 2017), 99-120.
[76] Ibid.,116-118.
[77] Orefice, 'I Big Data e gli effetti su privacy, trasparenza e iniziativa economica', (n.33) 106-107.
[78] Rodotà, 'Il mondo nella rete. Quali i diritti, quali i vincoli' (n.4) 25-26.
[79] Ibid., 29.

fundamental freedoms.[80]

Consequently, it can be understood how the information for the granting of consent, although structured in a way that is compatible with the recent Regulation, does not seem sufficiently effective to curb the increasing use of Big Data released in the market and its predictive potential, circumventing the perimeter of the rules on consent for the processing of personal data and lending itself to mostly formalistic applications.[81]

In any case, it is necessary to consider how the European legislative framework, although it does not directly contemplate Big Data, does establish some fundamental principles in the collection and use of personal information, and how recent rulings of the Court of Justice of the European Union remind us of the importance of effective data protection. Finally, the European Guarantor, in various opinions and initiatives, has not failed to underline the importance of a coherent regulatory application in the era of Big Data, developing the concept of protection of personal information and stressing the need to take advantage of the opportunities offered by new technologies, without allowing them to determine the social values of reference.[82]

In this context, the real problem arises from the lack of awareness that citizens have of how much of their privacy is for sale, of how invasive personalized advertising built from their clicks is in their lives and of how inadequate is the defense that current legislative systems really guarantee. to protect citizens and communities.[83]

The lack of full knowledge could also refer to the existence of second (or subsequent) uses of the data, as well as to the secondary information requested by the techniques of extraction of significant information from the data, capable of generating information different from that object of the original processing and used for purposes other than those expressed by it that, if they were unknown to the interested party, they would be unlawful as they were not expressly authorized.[84]

As regards the second uses of personal data, it will therefore be necessary to give specific consent for their processing, demonstrating full knowledge and desire for authorisation to carry out the processing: otherwise, the operations of processing personal data must be considered unlawful and contrary to art. 13 or, in the case of sensitive data, with art. 26 of the Legislative Decree. 2003/196 (Privacy Code) and with articles 13, 7 and 9 of European Regulation 2016/67987.

In the Internet of Things sector, there is also a real risk of unintentional activation of the smart device and, consequently, of unconscious transfer of the data flow generated by it, with an obvious loss of control of the information and of decision-making power over personal information by the user.[85]

---

[80] N M Richards, J King, 'Three Paradoxes of Big Data', (2013) 66 Stanford Law Review Online 41,42.
[81] Delmastro Nicita, 'Big data. Come stanno cambiando il nostro mondo ', (n. 13) 142.
[82] S Sica, V D'Antonio, G M Riccio, *La nuova disciplina europea della privacy*, (CEDAM 2016), 250-276
[83] Talia, 'La società calcolabile e i big data. Algoritmi e persone nel mondo digitale', (n.12) 48.
[84] Zanuzzi, 'Internet of things e privacy. Sicurezza e autodeterminazione informativa' (n.76) 111-112.
[85] , G Sartor, 'Privacy, reputazione, affidamento: dialettica e implicazioni per il trattamento dei dati personali', in U Pagallo (ed.), *Privacy digitale. Giuristi e informatici a confronto*, (Giappichelli 2005), 81-97.

Of great interest, then, is the Opinion 8/2014 of WP29[86] where it specifies that, for the processing to be considered lawful, it is necessary for the user to maintain total control of their data throughout the life cycle of the device.[87]

In reference to IoT and information technologies capable of activating invasive individual profiles that also affect sensitive user data. However, regulatory uncertainty seems to be accentuated given that Directive 2002/58 (Privacy Directive on the processing of personal data and the protection of privacy in the sector) should apply to the processing of personal data related to the provision of electronic communications. electronic communications services) whose provisions, developed in Articles. 32 and 32 bis and 121-132 of the Privacy Code, are currently under review since a proposal for a Regulation aimed at their repeal was presented.[88]

According to WP29, the critical issues mentioned could relate both to the nature of the smart object device and to a lack of coordination between stakeholders in the processing of personal data, in relation to the adoption of the minimum necessary security measures. In the first hypothesis, it could be appealed to the necessary compliance with the criterion of privacy by design, i.e. "privacy by design", expressed by art. 25 of EU Regulation 2016/679, which provides for the protection of personal data from the design of the processing, through a proactive and not merely reactive approach: this indication seems essential in relation to processing carried out with smart objects as it facilitates the protection of personal data It is an intrinsic component of the architectural structure of the device.[89]

In this regard, Article 32 of the Privacy Code, which obliges providers of electronic communications services to adopt technical and organisational measures appropriate to the existing risk in order to safeguard the security of their services and for the obligations referred to in Article 32 bis (i.e. for notifications in the event of a data breach). In the same line of guarantee of personal data, art. 24 of EU Regulation 2016/679, which refers to the principle of responsibility, referring to the set of measures that the controller and the processor must implement to guarantee and be able to demonstrate that the processing is carried out in accordance with this regulation, a criterion created with specific reference to economic-financial and final information, it seems but apt to cover the totality of the company's operations.[90] The guarantee of privacy by design and the principle of responsibility is then accompanied by respect for privacy by default, implemented by art. 25 of the Regulation, which establishes that, by default, only the personal data necessary and sufficient for each specific purpose of the processing and for the period strictly necessary for these purposes will be stored.[91]

This principle, as Franco Pizzetti points out, expresses an effective protection against the risk, particularly insidious and present in smart objects,

[86] WP29 distinguishes data processing consisting of its acquisition by the device manufacturer, or by another interested party, from processing related to its possible subsequent use.
[87] P Moro, C Sarra, *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, (FrancoAngeli 2017), 102.
[88] Ibid., 103-106.
[89] Zanuzzi, 'Internet of things e privacy. Sicurezza e autodeterminazione informativa' (n.76) 101.
[90] E C Pallone, 'Internet of Things e l'importanza del diritto alla privacy tra opportunità e rischi' (2016) 17 (55) Ciberspazio e diritto 163, 183.
[91] M Iasselli, *Diritto e nuove tecnologie. Prontuario giuridico ed informatico*, (Altalex 2016) 180-181.

of use of data by an indefinite number of subjects and for purposes other than those for which they were originally collected, even more so if it is carried out in an automated way and without the identification of a clear responsibility attributable to an identified owner.[92]

Finally, the criteria can be combined with Recital 78 of the Regulation (EU) 2016/679 which states that the protection of the rights and freedoms of natural persons in relation to the processing of personal data requires the adoption of appropriate technical and organisational measures to ensure compliance with the provisions of this Regulation. [93] Such measures could include, among other things, minimizing the processing of personal data, pseudonymizing personal data as soon as possible, providing transparency on the functions and processing of personal data, allowing the data subject to control data processing, and allowing the controller to create and improve security features.[94]

The Regulation will remain central even after the entry into force of the Regulation since the latter, as it does not contain a general regulation on security measures, would in any case refer to the content of Regulation 2016/679 and the EU Communications Code.[95] The challenge is to harmonize often contradictory interests and needs, such as transparency and confidentiality, managing to anonymize users without erasing the interest of the data collected, obtaining an appropriate balance between the logic of the market and the essential guarantee of prevailing and non-negotiable rights.[96]

Conclusions.

M C Bianca's insights on the topic of privacy remain highly relevant.[97] Once again, the urgency of an effective regulation of Big Data, and more generally, of the personal information that circulates on the network, inspired by constitutionally guaranteed values and aimed at protecting the individual from the improper use of information technologies, avoiding any possible de-responsibility attributed to the interpretative capacity of the algorithms used.[98] The algorithm describes crystallized thinking[99], a procedure capable of effectively solving a problem, of calculating a result, through a set of complementary steps, therefore, by maximizing, through the processing and analysis of the data found, the encounter between the demand and supply of

[92] F Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, (Giappichelli 2016) 288-290.
[93] A Maceratini, 'New Technologies, Big Data and Human Rights: An Overwiew', in A Caligiuri (ed.), *Legal Technology Transformation*, (Editoriale Scientifica 2020),11-20.
[94] Regulation (EU) 2016/679
[95] Orefice, 'I Big Data e gli effetti su privacy, trasparenza e iniziativa economica', (n.33) 121.
[96] See: 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 3, 23.
[97] G U Rescigno, F D Busnelli, C.M. Bianca,' La protezione dei dati personali. Commento al d.lgs. 30 giugno 2003, n. 196, Padova, 2007', (2008) 3 Diritto pubblico 1035,1042.
[98] Simoncini, Suweis, 'Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale', (n.40) 103.
[99] For more information, see the Statement *on Algorithmic Transparency and Accountability*, published by USACM, the American Association for Computational Mechanics, as well as the European Parliament Resolution on robotics of 16 February 2017.

information, algorithmic efficiency runs the risk of marginalizing processes and decisions linked to the real meaning of things to affirm a purely measurable.[100]

This is desirable for developing innovative delineation of models of active digital citizenship, as the foundation of effective freedom in the construction of personal identity.[101]

It is easy to understand how, bottom-up, this implies and entails the provision of a more equitable redistribution of information power on the Internet, capable of supporting unprecedented opportunities for relations between civil society and national and international institutions.[102]

In other words, the norms and procedures produced synergistically by technology and law become essential, an expression of an evolving techno-law, capable of sustaining the capacity for criticism and unexpected events, avoiding what Rodotà effectively described, highlighting all the risks to privacy, the freedoms of the person, the lack of consent in the use of data, as the dictatorship of the algorithm", as an emblem of a society of depersonalization. Moreover, "that history leads to the reign of human rights rather than the reign of Big Brother can only be the subject of a compromise.[103]

[100] B C Han, *Nello sciame. Visioni del digitale*, (Nottetempo 2015) 1 ff.
[101] A Maceratini, 'Privacy e informazione nell'era dei Big Data', XI (2019) 2 Tigor: Rivista di scienze della comunicazione e di argomentazione giuridica, 79,96.
[102] G De Anna, 'Automi, responsabilità e diritto', VIII (2019), n. *1Rivista di filosofia del diritto*, 125,142.
[103] S Rodotà, *Tecnologie e diritti* (Il Mulino 1995) 25-46.