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.

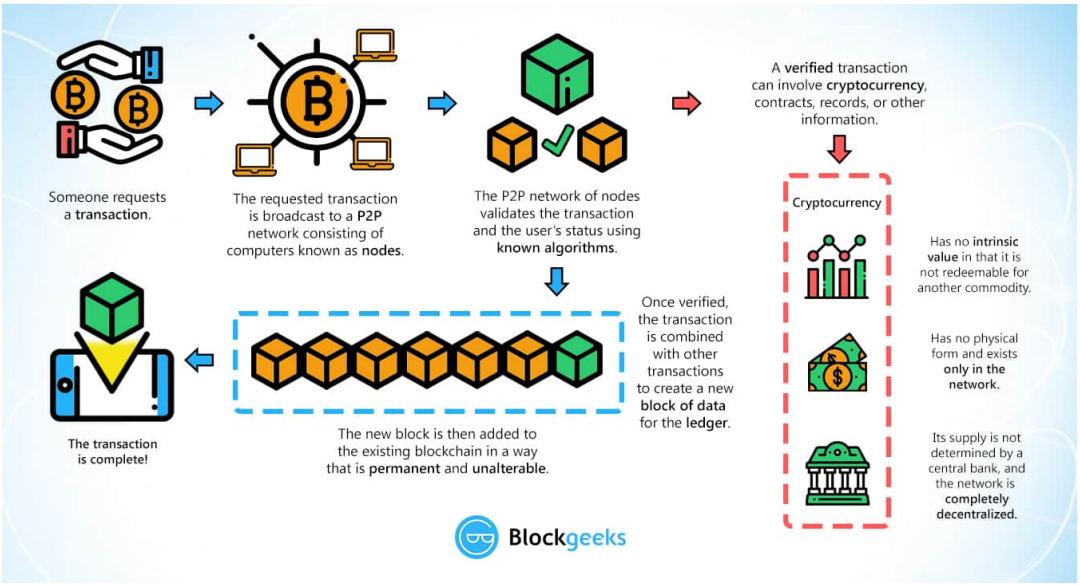
But a new technology seems to have generated a new climate of trust: the reference is to the blockchain which, not surprisingly, arises from a climate of distrust, even if referred to a different area, from that of data. On the occasion of the crisis of subprime mortgages, after, following the bankruptcy 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.

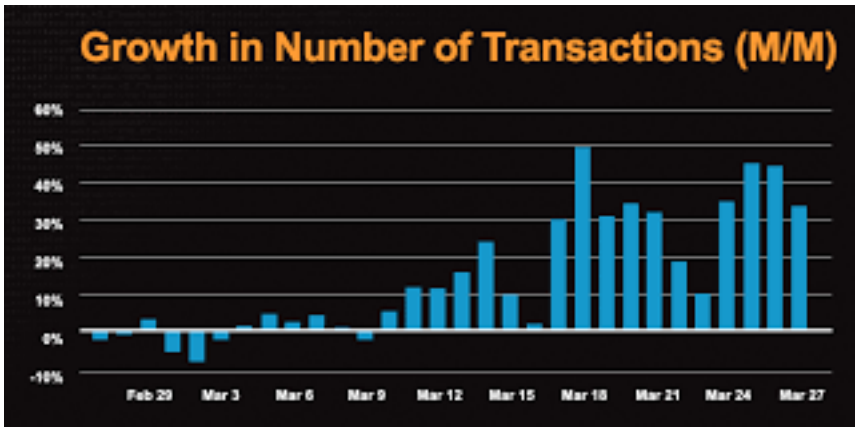
Conclusions: the world is not yet ready for complete digital disintermediation

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).