Sara Merla

REVISTA DIREITO MACKENZIE

ISSN: 23172622

BIG DATA AND LAW: GENERAL PERSPECTIVE ABOUT DIFFERENT NARRATIVES

Lara Merla*

RECEBIDO EM:	22.11.2019
APROVADO EM:	2.12.2019

* Ph.D Student at the Department of Law of the University of Turin (Italy).

2019 | v. 13 | n. 2 | p. 1-23 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212971

ABSTRACT: In the common era, the use of integrated technologies and connected devices even for domestic purposes is widely spreading. While the Internet of Things has helped improving everyday life standards, it has also increased the risks of exposing consumers to cybersecurity threats and to improper use of their personal data. The aim of this paper is to verify how the protection of consumers' privacy and the UE cybersecurity discipline can work together through a common path. Moreover, to underline that cybersecurity risks are an important factor which is taken into account by both societies and companies, as it does not only include the risk of a network data breach, but also the risk that the entire enterprise's business activities which rely on open digital connectivity and accessibility will be substantially undermined. This is even more important considering the huge amount of data that consumers provide on a constant basis via their connected devices. Such data does not only allow professionals to track users' profiles to provide the services they have requested, but it also influence their commercial choices. Poor cybersecurity of these devices, a substantial lack of effective control on the use which is made of the data obtained via them and a scarce awareness by consumers themselves, can lead to privacy infringements, risks to physical safety, and the widespread disruption of online services, which should and must be prevented both at a national and EU level.

KEYWORDS: Big Data, law, privacy, cybercrime, cybersecurity.

BIG DATA E LEI: PERSPECTIVA GERAL SOBRE DIFERENTES NARRATIVAS

RESUMO: Na sociedade contemporânea, o uso de tecnologias integradas e dispositivos conectados, mesmo para fins domésticos, está se espalhando amplamente. Embora a Internet das Coisas tenha ajudado a melhorar os padrões de vida cotidiana, também aumentou os riscos de expor os consumidores a ameaças de cibersegurança e ao uso indevido de seus dados pessoais. O objetivo deste trabalho é verificar como a proteção da privacidade dos consumidores e a disciplina de cibersegurança da UE podem trabalhar juntas por um caminho comum. Além disso, vale ressaltar que os riscos da cibersegurança são fator importante que são levados em conta tanto pelas sociedades como pelas empresas, uma

vez que inclui-se não só o risco de uma violação dos dados da rede, mas também de que as atividades empresariais, de toda a empresa, as quais dependem da conectividade e acessibilidade digitais abertas, sejam substancialmente comprometidas. Isto se torna ainda mais relevante quando consideramos a enorme quantidade de dados que os consumidores fornecem constantemente através dos seus dispositivos conectados. Esses dados permitem que os profissionais acompanhem os perfis dos utilizadores para fornecer os serviços, como também direcionam suas escolhas comerciais. Uma cibersegurança deficiente destes dispositivos, uma falta substancial de controle eficaz sobre a utilização dos dados obtidos por meio deles e uma escassa sensibilização dos próprios consumidores, podem acarretar em violações de privacidade, riscos para a segurança física do consumidor, bem como em perturbação generalizada dos serviços on line, que devem e devem ser evitados tanto a nível nacional como da UE.

PALAVRAS-CHAVE: Big Data, direito, privacidade, cibercrime, cibersegurança.

1. Introduction

This paper discusses the hard resilience of law against the on-going technological changes. Here, I propose the preliminaries of an ambitious project. In fact, on one hand, law has to take charge of technologically novel phenomena, like collection and exploitation of big data and development of Artificial Intelligence; on the other hand, this has to occur taking account of the loss of the jurist's authoritativeness with respect to other professionals who are able to handle computer languages, like coders or programmers[1].

After a brief foreword about the material transformation of the current conditions to show how the outcomes of the traditional discussion on the limits of formalism permit us to deal with these novel themes, the second paragraph will deal with the complicated relationship between collection and elaboration of big data and those fundamental rights that are more threatened by information and communication technologies (ICT), which are applied to all aspects of everyday life. A first overview of the collective dimension, that constitutes the matrix of big data and of how it can be

1 See, for a first overview, LESSIG, L., *Code and other laws of cyberspace*, Basic Book, 1999.

combined with the individualistic structure of western law, founded on the construction of subjective right, will be introduced.

In the third paragraph, we will deal with the right to privacy in the light of European Regulation 679/2016 highlighting a legal framework that is not able anymore to achieve the aim as a result of its structural bond with the legal entity holder of the power to give consent.

In closing (fourth paragraph), we will indicate what we think to be the main lines of future in-depth analysis aimed at illustrating a new conception of the right to privacy, which was taken into consideration in some way by European legislators during the discussion on European Regulation 679/2016, but then was not followed in the final approval. It is the elaboration of a concept of privacy as a digital common good, that is able to offer an institutional collective and transnational answer to a social question of computer security, produced by a technological and also collective and transnational challenge, which puts in check the dualism between the State and the individual, holder of (available or not) rights.

2. Law effectiveness put in check by the evolution of the current material conditions

This is not the place for analysis, even only hinted, of the current condition. It can be taken for granted that today law is "boundless"[2] and that the sovereign state has lost the monopoly on its sources. Nevertheless, the juridical space is still jealously kept separated from the political one and the economical one by the dominant thought.[3]

Positivist jurists build a self-legitimation strategy founded on the artificial scan of a material phenomenon, equal to the one relative to the way in which a social group governs itself. They participate as protagonists in "disciplining" the academic knowledge[4] by handing over to the *political scientist* the phase that precedes the formal validity of the rule (it's the political scientists who study the parliamentary processes and before that the electoral ones) and to the *sociologist* the study of its concrete effects.

2 See, for all, FERRARESE M. R., *Il diritto sconfinato. Inventiva giuridica e spazi nel mondo globale*, Edizioni Laterza, 2006.

3 See, about the explosive force of globalism, MONATERI, P. G., *Dominus Mundi, Political Sublime and the new World Order*, Oxford Hart Publishing, 2018.

4 See MATTEI, U., *Beni comuni. Un manifesto*, Edizioni Laterza, Bari, 2011.

Jurists place themselves between the before and the after, being good at hermeneutic techniques in which formalism and realism confront each other in a space that is protected by the impulses of the political material conditions. The debate about law effectiveness and especially about its bonds with different but linked questions, such as legitimacy and validity, articulates itself in this space. Here, some of the most important scholars of the 19th century, who have looked at the issue of the efficacy of a law that has been imposed from the top, confront each other. Among the eponymous heroes of these debates that involve the question itself of the law boundaries: Santi Romano, Carl Schmitt, Hans Kelsen, Herbert Hart. All these people, who are to such an extent historized that we can exempt ourselves from offering an even brief bibliography about their thought, interrogate themselves in-depth about law effectiveness. This requisite, directly linked in the space of their reflection to efficacy and validity, becomes even more crucial today with the coming of a global technology that is not governable within the boundaries of statehood.

To our ends, it suffices to register that the masters of positivism interrogate themselves about the mixture among legal orders and, in particular, between national and international law that, as is known, numbers among its sources also customary law, meaning factual behaviors repeated in time to which the community acknowledges compulsory nature. It is clear that the question of effectiveness turns out to be all the more conditioned by the transnational (or trans-state) dimension of law, which constitutes the most difficult challenge of the present compared to the historical period in which the masters of juridical positivism, in all its forms, worked. Plus, the transnational dimension is founded today on a technological transformation of the global connections, simply not thinkable in their time.

The transnational consuetudinary source, of primary importance today, permits us to affirm that with the coming of the new technologies law is still able to shape society only if indeed it is followed by the "global citizens" (rectius: global consumers).

Today, in fact, at a global juridical level, effectiveness is obtained by the top by transnational layouts, provided with authority and peremptory power5, able to conditionate the use of information technologies (e.g. World Trade Organization, ICANN and International Monetary Fund), or by the bottom through the working of social

5 See, for a critical reflection about the borrowed relationship between the juridical and the political in the global world, MONATERI, P. G., *Dominus mundi: Political Sublime and the World Order*, Oxford Hart Publishing, 2018.

movements, able to act directly on technology (e.g. Aron Swartz6 e and his Guerrilla Open Access Manifesto). But that's not all. The State, still able to exercise sovereign power at the time of Romano, Kelsen, Schmitt or Hart, turns out to be taken aback and in some way subordinate by virtue of a tendential technological inadequacy of its own bureaucratic structures. In other words, the State's legal order has to compete with information-regulation systems (competing if not directly conflicting and opposing) crucially advantaged by not having to care about legitimacy. To this, it has to be added that the technological transformation that has accompanied the globalization of markets (I'm using this term not to open the question of the cause-effect relationship) has determined an unprecedented disequilibrium in the balance of power between private capital and public bodies, in which setting the global factuality of law (in other words, the global custom) is all the more determined by communication technology (in private hands) that conditions or even determine individual behaviors. It's a *technological factuality* world the one that surrounds us, within which the positivist jurist, although sitting on the shoulders of giants, is completely disoriented.

3. Law (in)effectiveness in a world governed by Big Data

It is known that the hyper-connected technological society in which we live is founded on a detailed collective memory, without historical precedent. Billions of relationships that in the past did not leave any trace or were forgotten before long anyway (affecting only a reduced number of people) leave today indelible computer prints that permit social cooperation of global reach[7]. To become aware of this, it suffices to think how more data about our real life our smartphone or email know compared to us, and especially how these tools, save in exceptional cases, never forget anything (to forestall the loss of this memory, we willingly transfer our phone books and our chats into very powerful collective memories, called clouds, which are organized and governed by the big techno organizations, like Google or Facebook). Or, let's imagine how the payments that we make with a debit or credit card stay forever registered. So, these billion of prints that

6 SWARTZ, A., *Guerrilla Open Access Manifesto*, Archive.org, 2008.
7 See HARARI, Y. N., *Sapiens. Da animali a dèi. Breve storia dell'umanità*, Bompiani, 2017.

we leave in that big informatic space that bears the name of infosphere[8] have revolutionized, as writing and then printing have done before, our social organization, and this is exactly the new area from which the new capitalistic organization, which the jurist has to trample on, depends[9]. A very different area, of a far more global reach than the one, although rapidly changing itself, against which the masters of the past had to measure.

The incessantly growing collection of data, combined with the vertiginous decrease of their elaboration costs, has now made our lives available to all those who, for various reasons, make business with this[10].

Let's think about the data that every day we concede through platforms like Twitter, Instagram, Facebook to our friends, colleagues, employers and, of course, to the platforms themselves.

But let's also think about the less "recreative" uses of our data that, for a while already, are making us fear the development of a real control society, a dystopic nightmare that worried even Stefano Rodotà more than forty years ago.[11]

On the 24th of August in the far 1965, Gloria Placente, a 34-year-old from Queens, was driving to Orchard Beach, in the Bronx. Wearing shorts and sunglasses, married, the woman, was looking forward to enjoying a little relax on the beach. But just when she was crossing the bridge of Willis Avenue with her Chevrolet Corvair, she was stopped and surrounded by a dozen of policemen. There were also a hundred reporters, ready to witness the launch of the New York Police Department's new initiative, the operation CORRAL (Computer Oriented Retrieval of Auto Larcenists). Fifteen months before, Placente had run a red light and had not responded to the bench warrant, an infraction that CORRAL was about to sanction with an exemplary punishment that we could call techno-Kafquesque[12].

8 FLORIDI, L., *Infosfera. Etica e filosofia nell'età dell'informazione*, Giappichelli Editore, Torino, 2009; FLORIDI, L., *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

9 See MATTEI, U. & QUARTA, A., *The Turning Point in Private Law: Ecology, Technology and the Commons*, Elgar studies in legal theory, 2018.

10 About the structural change, caused by this reorganization, you can read the apologetic pages by ANDERSON, C., *The long tail: How endless choice is creating unlimited demand*, Random House, 2007. Even more interesting and documented are the critic ones by LANIER, J., *Who owns the future*, Published by Simon and Shuster, 2013; MOROZOV, E., *Silicon Valley: I signori del silicio*, Codice Edizioni, 2017.

11 RODOTA', S., *Calcolatori elettronici e controllo sociale*, Il Mulino, Bologna, 1973; LANIER, J., *Ten arguments for deleting your social media accounts right now*, 2018; LANIER, J., *Dawn of the New Everything: Encounters with Reality and Virtual Reality*, 2017.

12 SCHONBERGER, V. M. - KUKIER, K., *Big Data: A Revolution That Will Transform How We Live, Work and Think*, John Murray, 2013.

The operation was structured this way: a police car placed at the end of the bridge used to transmit the number plate of the approaching cars to an operator, sitting at a teleprinting miles away, who would insert it in a computer that would look for the number plate in a database of 100,000 stolen or belonging to known criminals vehicles. If a correspondence were found, the operator would alert a second patrol car at the other end of the bridge. Operation time: 7 seconds.

Compared to the extraordinary equipment with which today the police are provided, automatic recognition of the number plates, surveillance cameras, GPS trackers, operation CORRAL looks similar to a hunting trip in the Neolithic. Today, with over one and a half billion smart detectors that connect automatically to our mobile phone devices and other objects that operate in the so-called Internet of things (IoT), we can imagine a total capillary control over our movements. The automotive sector is emblematic of the transformations in action[13]: John Elkann, president of FCA and Ferrari, has declared that they are working together with Google on the fabrication of intelligent cars, the *self-driving cars*, and also Apple is doing business with self-driving cars and the creation of smartphones and intelligent glasses, provided with sensors to analyse whether the vehicle is moving and whether the person who is using the telephone at that moment is driving or not: if both conditions occur, the software stops the function of sending messages. Moreover, Intel and Ford are testing systems of facial recognition that, in case the driver's face is not recognised, would not only prevent the car from setting itself in motion but would also send a picture to the owner (bad news for the teenagers taking their parents' car without asking for permission).

But the uses of data are numerous, and police uses are just a little part, because, notoriously, the *business community* is way more imaginative than police bureaucracy. An example is given by the Barcelona Teatreneu: like many other - not only Spanish - cultural realities, this theatre had to deal with a revenue decrease after the government, broke and desperate for additional income, had raised taxes on ticket sales from 8 to 21 percent. The theatre management, nevertheless, found an ingenious solution: thanks to an agreement with the advertising agency Cyranos McCann, a tablet was inserted in

13 PALANZA, S., *Internet of Thinks, big data e privacy: la triade del fututo*, in Documenti IAI (Dipartimento Affari Internazionali), 2016, p. 3, available online: www.iai.it; PANETTA, F., *Harnessing Big Data &, Machine Learning Technologies for Central Banks, available:* www.bancaditalia.it BENKLER, Y., *The Penguin and the Leviathan: How Cooperation Triumphs over Self-Interest*, Published by Crown Business, 2011; BENKLER, Y., *The Political Economy of Commons*, 2003.

every seatback which is able to analyse the facial expressions of those sitting in the row behind. According to the new business model, there is a free entrance in the theatre, but the spectators will pay 30 cents for every laughter recognised by the tablet, with a maximum amount of 24 euros (equal to 80 laughter) per show.

So, the solution is either never to laugh, provided that you succeed, or to pay. The total gain for every ticket, by all accounts, has risen by 6 euros. From the point of view of the Silicon Valley, what we have just described is a perfect example of radical innovation (*disruption)*: the proliferation of intelligent sensors and Internet connections creates new business models and money flows. Obviously, the real value for the corporation is the deep knowledge of each spectator's tastes, which can be then elaborated in macro-types and used for advertising purposes.

The just described scenario should raise in the jurist many questions about what role the law takes in all this. In the first example, both the acquired evidence and the way in which it has been acquired are at stake, questions that interrogate the criminal procedure jurist and that we shall not examine here in-depth for reasons of space and convenience; the last example poses a problem on the contracts' nature (whether they are smart or not) also with regard to the essential elements and especially to the adequacy of the notion of consent as modern cornerstone of the institution. The agreement requisite traditionally founds and legitimizes contractual freedom[14]. In modern western law, these ideas, already present in natural law philosophy (and inserted in the codes by Domat) were systemized by the German romantic jurists, who impregnated them with the individualistic spirit asserted by Romanticism[15]. Namely, key importance was given to private will and freedom, so far as not to leave any more space to the so-called distributive justice, meaning the one realized with jurisdictional control on equity of the choices made by the parts. Even today, in private law lectures, students are taught the total irrelevance for the law of the motives that have driven to contract. The contracting parties became, therefore, free to establish with the contract the requisites they saw fit (save for those clauses that are clearly unfair). Of course, both the jurist and any citizens provided with common sense are aware that the typical *synallagma*

14 GANDONI, A., *Beyond the hype: Big Data concepts, methods and analytics*, International Journal of Information Management, Volume 32, Issue 2015, pp. 137-144; ELGENDY, M. & ELRAGAL, A., *Big Data Analytics in Support of the Decision-Making Process*, ScienceDirect, 2016.

15 MATTEI, U. & QUARTA, A., *The Turning Point in Private Law: Ecology, Technology and the Commons*, Elgar studies in legal theory, 2018.

of every contract is an "imaginary" abstraction, one of those invented structures on which social cooperation is founded. Indeed, the economic advantage or disadvantage generated by the contract cannot be reduced to the one related to the contracting parties, provided that the agreement can be found also indirectly, as the Teatreneu example fully highlights: the spectators' consent can be considered presumed at the moment of their entrance in the theatre for the show (not of the payment of the price, supposing that, since it is determined by the laughter, it is paid at the end of the show), but the civilly relevant analysis does certainly not stop here. In fact, the most economically significant relationship is not the one between the potential spectator and the theatre, but the one between the spectator and the owner of the algorithm that interprets the laughter. The theatre, then, not only determines unilaterally the ways of the synallagmatic contract but conditions the access to the theatre to the (unaware) transfer of sensitive data, such as preferences that are so intimate to determine a belly response like laughter, to a third party. It is not only the final use of these data (and their aggregation) unwittingly transferred in the form of a funny bet that stays in the shadow, but also the real beneficiaries of the "game" proposed by the theatre to its consumers. For the jurist, then, game and bet produce mere natural obligations; therefore, the spectator at the exit could refuse the payment (unless he authorized at the entrance the use of a credit card), which shows that the role played by traditional private law is almost irrelevant, since it is totally ineffective in business of this kind, almost fully governed by technological capabilities.

In fact, the contracts that we conclude with telephone operators or when buying technological devices pose unilateral clauses that, if not accepted, simply prevent the use of the devise, which is only formally owned by the holder (with relevant questions about the property's nature)16. These contracts, actually, force a transfer of sensitive data that constitute the real stakes, while jurists, given the changed balance of power, find themselves with no sharpened tools able to frame and discipline them.

For almost forty years, until the fall of the Berlin wall, Eastern Germany Stasi spied on millions of people, opened private letters and induced wives and partners to spy on each other, violating every kind of trusting bond and accumulating information, contained in 112 linear kilometres of documents. Almost thirty years after the fall, more data than ever about us are collected. We are constantly under surveillance:

16 MATTEI, U. & QUARTA, A., *op. cit;* MATTEI, U., *Trattato di diritto civile, La proprietà,* Utet, 2015.

when we use the credit card to pay, the mobile phone to communicate, the cart to do our shopping or the bicycle in sharing.

Jurists cannot suspend their critical sense, letting themselves be fascinated by the pleasure (real *circenses*) that our new Big Brother is offering us17. We should rather concentrate on the countless detrimental effects that we could see clearly when they were caused by the Stasi, but that we tend to underestimate when they are hidden by the seductive show society18. It seems convenient to summarize these criticalities in three macro-types: surveillance for marketing purposes; surveillance to judge, punish, and eventually anticipate criminal behaviours; effects of big data on the privacy of each of us, which is specific issue of this study.

Of course, the three types are interconnected because, from the topics that Twitter detects to be a matter of concern to us, elements about our occupation or personality useful for commercial purposes, as well as elements that can be used by the police for repression, justified by "crime prevention", can be inferred. It is difficult to imagine, as we will see, that, in these conditions, a global legal framework for privacy based on "consent" could return centrality to the law.

It is known that the private sector is surely not the only one to use confidently big data by taking advantage of the widespread technological illiteracy that has gradually turned us from subjects (citizens) to merchandise (our data)19. Governments also do this.

For example, according to an investigation headed by the "Washington Post" in 2010, it seems that the U.S. National Security Agency (NSA) intercepts and files everyday 1,7 billion among emails, calls and other communications between American citizens, and between them and foreigners.

But why collect all these data? The answer is connected to the way in which surveillance has developed in the era of big data. In the past, detectives used to apply tweezers to the phone wires to collect information about a suspect, aiming to know exactly that person. Today, the approach is different upstream: we use to say that "people *are* their information"20, the aggregate of their social relationships. This means that in order to study an individual in-depth analyst have to be able to access as comprehensively as possible the range of data that surround him, and involve, of course, many other

17 ORWELL, G., *1984*, Mondadori Edizioni, 2016.
18 DEBORD, G., *La società dello spettacolo*, Massari Editore, 2002.
19 About the transition from citizen to consumer to merchandise, see MATTEI & QUARTA, *op. cit.*
20 FLORIDI, L., *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

2019 | v. 13 | n. 2 | p. 1-23 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212971

people. Once, this was technically difficult and very expensive: today, it is simple and at almost zero cost. Since, in addition, the governments cannot know who the next suspects of terrorist attacks will be, we might as well store as much information as possible to be able to extract them, when necessary, with a computational force that increases exponentially, according to Moore's law[21]. Hence the development, especially in the most conservative states of America, of extending investigations.

Nevertheless, however worrying the ability of companies and governments to get their hands on our personal information might be, with the coming of big data an even more serious problem arises: the use of the previsions to judge us.

The opening scene of the film *Minority Report*[22] depicts a society in which previsions are so accurate that they enable the police to arrest individuals before they commit crimes. People are imprisoned not for what they have done, but for what they are going to do. As everyone knows, the film ascribes this preventive intervention of the public force to the *Precog*, individuals provided with extra sensorial powers of precognition, thanks to which the police can punish not the crime itself, but the mere intention to commit it.

A similar social organization would, obviously, demolish the bases of criminal law - for example, the notion of "attempt" under article 56 of the Italian Penal Code; in fact, for its fulfilment, it requires the manifestation in the real world of an intent in "suitable acts, aimed in a non-equivocal way", since the mere criminal purpose is not punishable. As authoritatively underlined by V. M. Schönberger[23], if the previsions that originate from big data were perfect, if the algorithms were able to foresee our future with absolute clarity, we would not have any freedom of action anymore and we would behave exactly as determined by the previsions. If perfect previsions could exist, they would deny human will, i.e. the necessary condition for all intentional crimes, hence for the overwhelming majority of those mentioned in the penal code. Paradoxically, perfect foreseeability would deprive us of the freedom of choice, this way relieving us of any responsibility. These are the disquieting ethical frontiers opened by our technologies that increasingly rebuild our cognitive paths in a way that is unquestionably (and maybe also completely) conditioned by the DNA sequences[24].

21 RIFKIN, J., *La società a costo marginale zero*, Volume 2097, Edizioni Mondadori, 2014.
22 SPIELBERG, S., *Minority Report*, Dreamworks, 2002.
23 SCHONBERGER, V. M. & CUKIER, K., *op. cit.*
24 MATTEI, U. & CAPRA, F., *The Ecology of Law: Toward A Legal System in Tune with Nature and Community*, Aboca Edizioni, 2015.

It is clear, then, that perfect previsions are (at the moment) impossible, as proved by the frontiers of theoretical science and quantum mechanics - which, in the world of the infinitely small, is entirely based on mere probabilities. The analysis of big data can foresee that a certain individual has a good chance of enacting a certain behaviour, but it suffices that it makes a mistake once to send an innocent to prison. Today, the error probability is statistically far higher than 11%. Nevertheless, since available data and computational ability keep increasing, systems such as Blue CRUSH and FAST are more and more used. While the first one indicates to the police officers the precise areas of interest, in terms of time and geolocation, where it is more probable that murders or blood facts occur, the second one tries to identify potential terrorists, monitoring their vital signs, such as non-verbal language or other aspects of the person (a sort of dangerous polygraph).

The room actually left free by jurists is conquered by those who are able to control technology, those who have the tools to understand it and forge it. Against this epochal change, the jurist, limited by the current tools and value apparatuses, ends up proposing rules that, in an attempt to discipline the use of big data and artificial intelligence, reveal themselves as obsolete even before landing in the courtroom.

4. Limits to the protection of the right to privacy between validity and (in)efficacy

Privacy is certainly the most debated problem opened by big data among jurists and computer experts.

At this point, a terminological and methodological clarification is needed: when we speak of big data, usually we do not mean personal data, but anonymized or, at least, pseudonymized or inferred data, not ascribable to the individual person involved by the data, or, in a second case, data that

> *can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*[25].

25 Art. 4 GDPR 2016/679.

2019 | v. 13 | n. 2 | p. 1-23 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212971

Actually, all this is partially true, since not all big data contain personal information, but certainly, the biggest part of the data that are generated today and then reused effectively include information of personal nature, and corporations have several incentives to acquire more of them, to conserve them for a longer time, to lead them back to the subject to whom they refer, and to reuse them. Furthermore, the data could also not be configurated as personal information, but, with data-processing, they can easily lead back to the individuals to whom they refer, as far as to deduce intimate details of their life. Let's think about users' management. "Smart" electricity meters that collect data for the whole day, with a frequency as high as 6 seconds, are being introduced, and, furthermore, the way the electrical equipment recalls energy creates, in technical jargon, the so-called specific "consumption signature": a boiler requires a different quantity of energy from the one required by a PC or by a lamp used to cultivate marijuana plants. The domestic use of electrical energy certainly reveals confidential information.

Yet, the question we ask ourselves here is not whether big data increase the risk for privacy (this is undisputed), but whether they modify the nature of risk and, therefore, the solutions[26].

As discussed in the previous paragraph, one of the many rights, and maybe the most crucial one, concerned by a massive use of new technologies is certainly the right to privacy, in both its meanings of (1) right to secrecy and (2) right to protection of personal data. As it is known, such distinction is highlighted by the Charter of Fundamental Rights of the European Union that dedicates two different articles to it, respectively art. 7, entitled "Respect for private and family life", and art. 8, entitled "Protection of personal data".

Of course, the two rights are intrinsically connected[27]. European (and domestic) legislation, which followed over the years, is hefty and certainly more geared toward the protection of civil liberties if compared, for example, to the American one[28]; nevertheless, the protective aspiration, if founded on inadequate juridical structures, can scarcely be considered a measure of success.

26 ZENO-ZENCOVICH, V. & CODIGLIONE, G., *Ten Legal Perspectives on the "Big Data Revolution"* Editoriale Scientifica, 2017.

27 See, in this regard: RODOTA', S., *Vivere la democrazia*, Edizioni Laterza, 2018; RODOTA', S., *Il diritto di avere diritti*, Edizioni Laterza, 2013; RODOTA', S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Edizioni Laterza, 2014; RODOTA', S., *Intervista su privacy e libertà*, Edizioni Laterza, a cura di Conti P., 2005; RODOTA', S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Edizioni Laterza, 2004.

28 FOCARELLI, C., *La Privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015; D'ACQUISTO, G. & NALDI, M., *Big Data e privacy by design*, Giappichelli Editore, Torino, 2017.

The need to harmonize the privacy laws of the various European countries led to the approval, in May 2016, of the European Regulation 679/2016, called in short General Data Protection Regulation, which came into force on May 25, 2018. The Regulation, directly applicable in all EU member states, extends its regulatory environment also to businesses situated beyond the borders of the Union that offer services or products to natural persons who find themselves in EU territory. This for the first time and in order to prevent the strictest European privacy laws from being eluded by simply moving business abroad. This is one of the many criteria chosen by the legislator to put into effect the compliance with EU parameters, trying to remedy the structural advantage of transnational corporations over states that we previously presented. The second element, driven by the search for effectiveness, is given by the principles of *privacy by design* e *privacy by default*, sanctioned by art. 25 par. 1, entitled: "Data protection by design and by default", where the meaning of this principle is clarified in these terms:

> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Furthermore, expressing the principle of *privacy by default*, it disposes of: "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."

In enunciating these two principles and in other regulatory provisions, as well as in the recitals, the European legislator proves to be rather careful in the provision for effective protection, even when he starts by saying *"Taking into account the state of the art, the cost of implementation..."*, avoiding, therefore, to put rules that, for the difficulty of implementation or the impossibility of financial means, end up remaining confined to paper.

2019 | v. 13 | n. 2 | p. 1-23 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212971

Nevertheless, setting the requirement of *privacy by design* in the hands of the subjects who process data, the new Regulation devolves, in fact, the regulatory part at the bottom of the process to the programmers of computer systems who, creating "privacy proof" software, replace the jurists in putting up the regulatory system. This means that new subjects, without juridical knowledge, give legitimacy to effective practice, by validating its rules. The algorithm becomes, this way, of substantial source of law, while the computer engineer replaces the jurist as a holder of hidden legislative power[29].

This is not the place to linger in detail on the new legislation since we intend to offer here a simple problematic catalog, showing how effectiveness, meant especially as efficacy but also as the validity of the rule of law, is being challenged by the new layouts.

One of the European legislator's strongest criticism[30] has concerned focusing, once again, data processing on the juridical basis of consent, which, although serving on paper as a residual criterion, in reality, in my opinion, is too frequently used. In fact, already the directive 96/45/EC provided for consent as a fulcrum for any large-scale sensitive personal data processing. The same is recalled by the Regulation that, on the basis of the definitions borrowed from the old directive, establishes in art. 4 par. 11 that consent has to be freely given, specific, informed and unambiguous, as well as liable to be proved by the holder of the processing (former art. 7 par. 1).[31]

This passed-on setting shows itself to be silly, or in any case unwilling to intervene on the authentic structural transformations produced by big data and by technological evolution, by now able to impact also sensitive data - think of biometric or genetic data, for instance.

The requirement of specificity, which requests that consent is given for every single processing, and the fact that it has to be informed, meaning that the person concerned has to know the current use and all the future uses, liquefies against companies and firms that process heterogeneous data, collected in a heterogeneous way, conserved and then reused for future processing, not necessarily foreseen nor foreseeable at the moment of the collection.

29 GAMBARO, A., *Il successo del giurista*, Il Foro Italiano, Vol. 106, No. 3, marzo 1983.

30 In this regard, see PIZZETTI, F., *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 46/95 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016.

31 Art. 4 par. 11 establishes that the consent of the person concerned 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*".

In order to avoid easy criticism about the technical difficulties in requesting a consent founded on such requirements, the European legislator, then, lists, under art. 6, which is about lawfulness of processing, a series of requirements, of which at least one is necessary to make personal data processing licit. These requirements, such as compliance with a legal obligation, the performance of a contract, a vital interest and so on, make the basic principle of informed consent, already very weak itself, residual and necessary only in case one of the other requirements does not subsist.

The requirement of consent, linked as it is to a dated conception of proprietary individualism, poses problems also in regard to *small data* and especially to those data that the new law defines under art. 9 as special categories of personal data, of which sensitive data are part, meaning:

> 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.

In principle, there is a prohibition to process such data, except when even only one of the requirements, sanctioned under par. 2, subsists, of which the first one is, indeed, the explicit consent of the person concerned.

There is, then, a second category of data whose processing is legitimate only in the presence of given requirements, meaning judicial data, especially if related to criminal convictions and crimes under art. 10 of the Regulation, for which, obviously, the subject's consent does not serve as a necessary requirement for the processing.

On top of that, in early 2018 the European legislator proposed a second Regulation, to flank the GDPR, called "Free flow of non-personal data Regulation". Such a source of law is, of course, addressed to the companies and multinational corporations that intend to process data for purposes that vary from marketing to advertising and only indirectly concern private subjects. The goal says the Commission[32], is to encourage the creation of a European economy of data and their use by *cloud computing* firms, a tool that has an immense ability to file, share and reuse data.

32 The document, available on the website of the European Commission, is entitled: "*A framework for the free flow of non-personal data in the European Union*", dated 19.09.2017, Brussels.

2019 | v. 13 | n. 2 | p. 1-23 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212971

In reality, it is known among the insiders that this is motivated largely, although hiddenly, by police reasons. The creation of filing places situated in EU territory makes the companies holders of data free to delocalize the holding of their own data also in other European countries (until now, in fact, Italian public authorities were obliged to file data only on Italian territory), facilitating, this way, international cooperation in crime prevention - *cybercrime*, in particular. The *cloud* or similar service providers will be, in fact, always obliged to communicate to state police authorities the data files in their systems, making it easier to find data and, therefore, catch the guilty party.[33]

5. A juridical answer to the Big Data's challenge: privacy as digital commons

In today's "zettabyte age", ICT allows huge computing power, producing huge quantities of data[34]. Such data are produced by all network users in a generally open and, therefore, "democratic" way; however, they are not used as openly and democratically, as we have seen. As if by magic, the individual prints that each of us leaves indelible on the net, exactly like those of Neil Armstrong on the moon, immutable since 1969, are aggregated and become collective entities, with an aggregate value that transcends by far the one of the parts that compose it. These collectives, which make it more and more easy to descend to their individual parts, determining even their behaviors, statistically foreseeable, exactly as in the world of the infinitely small, cannot be governed with the traditional tools of law, i.e. with those that have produced, following a historic evolution as long as modernity, the conditions of liberal constitutionalism, in which we still have the illusion to live.

In the current phase, capitalism is cognitive[35] and the Network not only creates its technological conditions but represents the space in which ideas, opinions, and political fights are shared. We know how the technological ability to use internet, *socials* and big data represents an imposing force in reaching and even determining the preferences of the active electorate or dusting with democracy the selection of the passive one (just think of the much debated Rousseau platform of the Five Star Movement in Italy).

33 See footnote 24 *supra*.

34 FLORODI, L., *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

35 MATTEI, U., *Beni comuni, un manifesto*, Editori Laterza, Bari, 2011.

The collectives are formed in the net with absolute simplicity, by reuniting people with similar characteristics or tastes, or simply because they inhabit bordering places; think for instance of the creation of group chats, created after the ideation of instant messaging platforms like WhatsApp. Obviously, they are extremely fluid aggregates, but very meaningful for whoever holds the control on algorithms, able to elaborate them in real-time. The (collective) subjects, holders of these abilities, can put in place actions of "micro-management" of our subjectivity, turning the information into suggestion,[36] or confining us in those that in computer jargon are called *filter bubbles* - in this regard, the Cambridge Analytica case caused a certain stir.

The objective is not clear to the user consumer and it does not even mean that there is a different goal from simply connecting people in order to extract the economic value of cooperation, which represents the corporation's structural vocation.

Luciano Floridi, the renowned philosopher of the University of Oxford who has been exploring for years the big data's potentiality, affirms that, in a world characterized by over-information, the interest of multinational corporations, but also of governments', is not linked anymore to *targeting*, meaning the profiling of the single individual, because it would be too complicated and little profitable. Today, the strategy is *group-targeting*, meaning the division of people in groups, on the basis of proved common preferences or choices. The group is not only politically but also economically stronger than the individual: only jurists, today still prisoners of the humanistic ideology typical of modernity, insist on the juridical protection of the individual - this way making weaker the weapons with which the "juridical" tries to rule the processing that transforms the present. Hence, the dramatical crisis of juridical effectiveness, formally legitimated, from which this paper started.

If factuality is collective, the search for legitimacy is still to the contrary (think of the individual's informed consent), with all the criticalities that we have tried to highlight in this paper. On the one hand, the personality of each of us is of significance if it is inserted in a group, but, on the other hand, the European and national legislators still define privacy as a subjective right, individually actionable in court. This *dyscrasia* is not only linguistic but affects law itself, since more and more frequently, by violating individual privacy, we also trespass on the privacy of other people, showing dramatically the

36 LANIER, J., *You Are Not a Gadget: A Manifesto*, Published by Knopf A. A., 2010; LANIER, J., *Who Owns the Future*, Published by Simon and Shuster, 2013.

2019 | v. 13 | n. 2 | p. 1-23 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212971

insufficiency of the monadic model. For example, by violating art. 7 of the Charter of Fundamental Rights of the European Union, also the private sphere of the people who live with the injured subject is invaded at the same time, and, with regard to the constraints of kinship, genetic data are the most paradigmatic example. The GDPR defines genetic data as: "*personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person...*". Genetic characteristics pose quite a few problems in terms of protection of personal data. They are part of particular meaning sensitive, data typology, and, therefore, their processing is, in principle, forbidden, as sanctioned by art. 9 par. 1, except one of the elements listed in par. 2 subsists. In any case, they show how the informed consent model is absolutely inadequate from the structural point of view. In fact, also in the absence of a privacy violation, meaning following an informed consent actually given by an individual, the latter involves necessarily also positions of other people with whom, in factual reality, the individual is intrinsically connected. Nor are we talking about small circles of relatives only. Recently, a group of scholars has published in *Science* a study that proves how anonymous genetic information, granted by millions of Americans who accept free test offers lured by the promise of knowing better their own genes, combined with context big data and a simple DNA sample (a hair found somewhere) can lead to the individuation of its holder, even if the latter has never done the test![37]

Defining the lines of a *pars costruens* of a vision of privacy authentically aware of our own identity's deep relational structure would go far beyond the extent of this paper, which does not want to be anything more than a problematic review. Today, the obsolete nature of every mechanistic epistemology that imagines society as the result of the algebraic sum of individual monads has been extensively denounced also in law[38]. We are relationship and social media have made this very clear. By permitting the processing of my personal data, I automatically involve also my "friends", whether they are or are not holders of an account. To think about privacy (as well as about many other juridical institutions) in a way that is structurally appropriate for a world that is moving more and more toward its virtual frontier, we need a jurist that is able to master the systemic thought[39] and a deeply relational and collective vision of the social

37 Science Magazine. Millions *of Americans Could Be Identified Using Genetic Databases, even if they have never taken a DNA test*, 14.10.2018.

38 See CAPRA & MATTEI *op. cit.*

39 CAPRA, F. & LUISI, P.L., *Vita e natura. Una visione sistemica*, Aboca Edizioni, 2017.

experience of which law cannot take charge if it stays prisoner of its nineteenth-century individualism. A 4.0 privacy can develop only by returning effectiveness to the law, deeply transformed by technology itself. This requires a serious reflection about common as a collective institution, able to offer resiliency against the concentration of global power.[40] Only a jurist able to embark in this endeavour will not abdicate his own role, nor will he become replaceable by the coder and by the algorithm. The first studies about privacy as access seem to move (shyly) in this direction.

6. Conclusions

In a movie of 1998, *Enemy of the State,* Robert Clayton Dean is a young lawyer of Baltimore that gets involved in a dangerous game: the NSA seeks him because thinks he knows dangerous information for national security and for this reason he is subjected to a special surveillance system that will make impossible his life.

The movie explains very well how the surveillance system, created for his security, it became, in reality, his death. Dean is under NSA control all the time and he still hasn't a private life. In a certain moment of the movie, there is a sarcastic joke: "*Privacy? It died 30 years ago. The only privacy that still exist it is in your mind, and maybe not even that*". (DEAN, 1998). A pessimist vision but for sure not too far from reality.

In recent years, privacy has been heavily damaged to protect what is called national security, public security and so on.

The surveillance systems of our cities are even more sophisticated; for this reason, Kenneth Laudon, a famous scholar ad expert of privacy wrote:

> My electronic image in the machine can be even more real than me. It is complete, always recoverable and predictable in statistical terms. I have a problem and I don't know what can I do. The machine knows what I can do. So, my reality is minus real then my registered image. This made me belittles (LAUDON, 1986).

One of the most important evidence that the privacy policies should always keep in mind is that the surveillance is linked to power: it is a means by which totalitarian

40 QUARTA, A. & SPANO', M., *Beni comuni 2.0. Contro-egemonia e nuove istituzioni*, Mimesis, 2016.

governments, of past and present, control how people act and what they think in order to check them every time.

This kind of practices helps to emphasize the existing social division. For this reason, it is hoped that people and institutions find a collective way to get back their identities and a new social interaction awareness favoring personal relationships to abstract communications on the web.

BIBLIOGRAPHY

ANDERSON, C., *The long tail: How endless choice is creating unlimited demand*, Random House, 2007.

BENKLER, Y. *The Political Economy of Commons*, 2003.

BENKLER, Y. *The Pinguin and the Leviathan: How Cooperation Triumphs over Self-Interest*, Published by Crown Business, 2011.

D'ACQUISTO, G.; NALDI, M., *Big Data e privacy by design*, Giappichelli Editore, Torino, 2017.

DEBORD, G. *La società dello spettacolo*, Massati Editore, 2002.

CAPRA, F.; LUISI, P. L. *Vita e natura. Una visione sistemica*, Aboca Edizioni, 2017.

ELGENDY, N.; ELRAGAL, A. *Big Data Analytics in Support of the Decision Making Process*, Sciencedirect, 2016.

FERRARESE, M. R. *Il diritto sconfinato. Inventiva giuridica e spazi nel mondo globale*, Edizioni Laterza, 2006.

FLORIDI, L. *Infosfera. Etica e filosofia nell'età dell'informazione*, Giappichelli Editore, Torino, 2009.

FLORIDI, L. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

FOCARELLI, C. *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015.

GAMBARO, A. *Il successo del giurista*, Il Foro Italiano, v. 106, n. 3, marzo, 1983.

GANDONI, A. *Beyond the hype: Big Data concepts, methods and analytics*, International Journal of Information Management, v. 32, Issue 2015, p. 137-144.

HARARI, Y. N. *Sapiens. Da animali a dèi. Breve storia dell'umanità*, Bompiani, 2017.

LANIER, J. *Who owns the future*, Published by Simon and Shuster, 2013.

LANIER, J. *You Are Not a Gadget: A Manifesto*, Published by Knopf . A., 2010.

LANIER, J. *Dawn of the New Everithing: Encourters with Reality and Virtual Reality*, 2017.

LANIER, J. *Ten arguments for deleting your social media accounts right now*, 2018.

LESSIG, L. *Coder and the other laws of cyberspace*, Basic Book, 1999.

MATTEI, U. *Trattato di diritto civile. La Proprietà*, Utet, 2015.

MATTEI, U. *Beni comuni. Un manifesto*, Edizioni Laterza, Bari, 2018.

MATTEI, U.; CAPRA, F. *The Ecology of Law: Toword A Legal System in Tune with Nature and Community*, Aboca Edizioni, 2017.

MATTEI, U.; QUARTA, A. *The Turning Point in Private Law: Ecology, Technology and the Commons*, Elger studies in legal theory, 2018.

MONATER, P. G. *Dominus Mundi. Political Sublime and the new World Order*, Oxford Hart Publishing, 2018.

MOROZOV. E. *Silicon Valley: I signori del silicio*, Codice Edizione, 2017.

ORWELL, G. *1984*, Mondadori Edizioni, 2016.

PALANZA, S. *Internet of Things, big data e privacy: la triade del future*, in Documenti IAI (Dipartimento Affari Internazionali), 2016, p. 3.Avaiable at: www.iai.it

PANETTA, F. *Harnessing Bid Data & Machine Learning Technologies for Central Banks*, Available at: www.bancaditalia.it.

PIZZETTI, F. *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 46/95 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016.

QUARTA, A.; SPANO' M. *Beni comuni 2.0. Contro-egemonia e nuove istituzioni*, Mimesis, 2016.

RIFKIN, J. *La società a costo marginale zero*, v. 2097, Edizioni Mondadori, 2014.

RODOTA', S. *Calcolatori elettronici e controllo sociale*, Il Mulino, Bologna, 1973.

RODOTA', S. *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Edizioni Laterza, 2004.

RODOTA', S. *Intervista su privacy e libertà*, Edizioni Laterza, a cura di Conti, P., 2005.

RODOTA', S. *Il diritto di avere diritti*, Edizioni Laterza, 2013.

RODOTA', S. *Il mondo nella rete. Quali i diritti, quali i vincoli*, Edizioni Laterza, 2014.

RODOTA', S. *Vivere la democrazia*, Edizioni Laterza, 2018.

SCHONBERGER V. M.; KUKIER, K. *Big Data: A Revolution That Will Transform How We Live, Work and Think*, John Murray, 2013.

SCIENCE MAGAZINE. *Millions of Americans Could Be Identified Using Genetic Databases, even if they have never taken a DNA test*, available online at the date 14.10.2019.

SPIELBERG, S. *Minority Report*, Breamworks, 2002.

SWARTZ, A. *Guerrilla Open Access Manifesto*, Archive.org, 2008.

ZENO-ZENCOVICH, V.; CODIGLIONE, G. *Ten Legal Perspectives on the "Big Data Revolution"*, Editoriale Scientifica, 2017.