Legal Technology Transformation

A Practical Assessment

Edited by

Andrea Caligiuri

Editoriale Scientifica

2020

LEGAL TECHNOLOGY TRANSFORMATION
A PRACTICAL ASSESSMENT

Edited by
ANDREA CALIGIURI

EDITORIALE SCIENTIFICA

2020

PROPRIETÀ LETTERARIA RISERVATA

© Copyright 2020 Editoriale Scientifica s.r.l.
Via San Biagio dei Librai, 39 – 80138 Napoli
www.editorialescientifica.com – info@editorialescientifica.com

ISBN 978-88-9391-985-2

SCIENTIFIC COMMITTEE

GUIDO LUIGI CANAVESI
Department of Law
Università di Macerata

GIUSEPPE CATALDI
Department of Social Sciences and Humanities
Università di Napoli "L'Orientale"

LIU HUAWEN
Institute of International Law
Chinese Academy of Social Sciences

MONICA STRONATI
Department of Law
Università di Macerata

CHRISTOPH VAN DER ELST
Tilburg Law School
Tilburg University

TABLE OF CONTENTS

PART III
ARTIFICIAL INTELLIGENCE AND SMART CITIES

PART IV
LEGAL RAMIFICATIONS OF BLOCKCHAIN TECHNOLOGY

SECTION I
BLOCKCHAIN AND CRYPTOCURRENCIES

NEW TECHNOLOGIES, BIG DATA AND HUMAN RIGHTS: AN OVERVIEW

ARIANNA MACERATINI

SUMMARY: 1. Big Data in the Information Society. – 2. Big Data. – 3. Big Data and Privacy. – 4. Big Data and Information.

1. *Big Data in the Information Society*

In the new economy, information is a fundamental economic resource that optimizes the relationship between supplier and user, for the loyalty of the latter.[1] The delineation of individual profiles and preferences will, in turn, contribute to influencing subjective behavior as significantly demonstrated by the phenomena of anticipatory shipping and anticipatory selling, developed by Amazon, capable of anticipating and inducing, apparently without forcing, the future customer purchases.[2] In this direction, also indicated by Opinion 8/2014 on the Recent Development on Internet of Things of Article 29 Data Protection Working Party (hereinafter "WP29"),[3] it is evident that the pervasiveness of information technologies, mainly of the Internet of Things,[4] has facilitated digital surveillance practices, making anyone who uses a computer device connected to the network easily

[1] J. Rifkin, *L'era dell'accesso* (Mondadori 2001), 65.

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

[3] WP29, Opinion 8/2014 on the Recent Developments on the Internet of Things, WP223, 16 September 2014. On this argument, S. Palanza, *Internet of things, big data e privacy: la triade del futuro* (IAI 2016) 18 ff.

[4] The Internet of Things (hereinafter "IoT"), an expression coined by the 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, see Palanza (n 3), 2. The identification of interconnected objects occurs mostly through a unique identifier, recognizable in radiofrequency, M. Iasselli, 'Privacy e nuove tecnologie', in M Iasselli (ed.), *Diritto e nuove tecnologie. Prontuario giuridico ed informatico* (Altalex 2016) 121 ff., 153 ff. Radiofrequency identification (hereinafter "RFID") is based on the use of microprocessors connected to an antenna, used as identification labels – *intelligent labels* – and capable of transmitting, via radio waves, signals readable by special readers; see ibid., 135. It should be noted that RFID has recently been joined by the massive use of Near Field Communication (hereinafter "NFC"), technologies that provide two-way and short-range wireless connectivity; see Palanza (n 3). On the impact of RFID on the exercise of individual freedom rights and on the protection of personal data involved in this kind of electronic processing, the European Data Protection Supervisor (hereinafter "EDPS") had already pronounced with an opinion of 20 December 2007 concerning the guarantees in the use of smart labels (EDPS, 'Opinion on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework (COM(2007) 96)', 20 December 2007), as well as the Commission of the European Communities with the Communication 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework', COM(2007) 96 final, 15 March 2007, outlining a political line that has as its objective the difficult reconciliation between the enhancement of the technologies and the protection of privacy, underlining the risks to health and the environment deriving from their use.

traceable and monitored by dealing – in some cases even without the data subject being aware of it, for example due to a sudden activation of the device used[5] – personal data, including information of a sensitive nature which, at a later time, could be aggregated to others allowing a more or less defined profiling of the interested party.[6] In fact, it should be noted that the data analyzed individually may not be particularly significant, but, if examined with suitable information technologies and in large volumes, they lead to the delineation of models and trends, capable of producing knowledge. It is therefore possible to intend how the term "personal data" is to be understood, following the direction of the 2013 OECD Guidelines[7] in an evolutionary and extensive key.[8] In any case, the massive processing of information marks the transition from a purely individual dimension of personal confidentiality to a collective dimension of the protection of personal data, in which the subject of informative self-determination becomes the entire community,[9] in the firm resolution to subtract from exclusive domain of the market information that constitute and guard the core of fundamental rights.[10]

2. *Big Data*

In the aforementioned OECD definition, all content generated by users on the Internet is Big Data, including blogs, photos, videos, behavioural data, social data, geolocation data, demographic data and identification data in general: contents that allow individual identification or which provide information on typed patterns of

---

[5] Palanza (n 3), 15.

[6] Iasselli (n 4), 135. In Italy, the regulation of the protection of personal data is contained in the Legislative Decree No. 196/2003, Privacy Code, aimed at bringing together the innumerable provisions of the sector which have occurred over the years and at introducing the most significant innovations of the Italian Data Protection Authority and of the European Directives on the confidentiality of electronic communications. Among the latter, it is necessary to mention the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, a provision recently repealed by General Data Protection Regulation (EU) 2016/679 (hereinafter "GDPR"); Legislative Decree No. 101/2018 adapted the Privacy Code to the provisions of GDPR. The current meaning assumed by privacy, by individualistic and substantially passive protection of the right to be left alone with the right to full control of information concerning us, is also sanctioned by the Charter of Fundamental Rights of the EU, which in Art. 8 provides for the right to the protection of personal data, as well as the Italian Declaration of the Internet Rights, published on 13 October 2015 during an international conference held at the Sala della Regina in Palazzo Montecitorio, S. Rodotà, *Il mondo nella rete* (Laterza 2012) 31.

[7] OECD Guidelines governing the protection of privacy and transborder flows of personal data (2013) <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. See Palanza (n 3), 8. It should be noted that the *ePrivacy Regulation* proposal of the European Commission (COM/2017/010 final – 2017/03 (COD), 10 January 2017) included in the category of metadata all data other than content, but only those processed on the network and not also data processed on devices, as also noted by the European Data Protection Supervisor, 'Opinion 6/2017 – EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)'.

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

[9] M. F. De Tullio, 'La privacy e i big data verso una dimensione costituzionale collettiva' (2016) Politica del diritto 641.

[10] Orefice (n 8), 141.

individual behaviour.[11] Big Data can also be described by means of the so-called 4Vs, that is, *volume*, as they are present in large quantities; *variety*, as they come from heterogeneous sources; *velocity*, since the data is analyzed through sophisticated algorithms that lead to a decision in real time;[12] *value* assumed, in this way, by the data.[13] It should be noted that most of this data is usually unstructured, that is, acquired and stored according to criteria different from those that oversee the organization of traditional electronic archives:[14] the peculiarity and potential of Big Data, capable of leading to a paradigm shift in the analysis of information,[15] are found in not having been extrapolated from representative samples by complex procedures,[16] but from the whole population observed, so that, in exploiting any possible correlation, in terms of predictive efficacy, their quantity prevails over the accuracy of the analysis procedure.[17] In Big Data analysis, then, predictions appear more significant than the information consciously released by users[18] making the same traditional distinction between personal data and non-personal data overcome.[19] An efficient use of Big Data, using Data Mining[20] or the latest Business Analytics[21] tools both paid, through the use of a particularly high number of variables that sometimes makes it difficult even to reconstruct the logic of the decision-making process,[22] to find hidden patterns and predictive rules,[23] represents for companies a critical as an undoubted competitive advantage,[24] provoking widespread entrepreneurial

---

[11] M. Delmastro and A. Nicita, *Big data. Come stanno cambiando il nostro mondo* (Il Mulino 2019), 35.

[12] For a useful definition of the algorithm, its characteristics and properties, A. C. Amato Mangiameli, *Informatica Giuridica. Appunti e materiali ad uso di lezioni* (Giappichelli 2015), 132-134.

[13] Delmastro and Nicita (n 11), 25-29; For an up-to-date delineation of Big Data requirements, M. Palmirani, 'Big data e conoscenza' (2020) Rivista di filosofia del diritto 77.

[14] Delmastro and Nicita (n 11), 10.

[15] A. Simoncini and S. Suweis, 'Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale' (2019) Rivista di filosofia del diritto 92.

[16] A. C. Amato Mangiameli, 'Algoritmi e big data. Dalla carta sulla robotica' (2019) Rivista di filosofia del diritto 112.

[17] Orefice (n 8), 149 ff.

[18] Delmastro and Nicita (n 11), 36.

[19] Ibid.

[20] For a complete analysis of the problems of *Data Mining*, C. Sarra, 'Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining', in P. Moro and C. Sarra (eds), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica* (Franco Angeli 2017) 41 ff. On the use of neural networks and of supervised and unsupervised learning algorithms, Amato Mangiameli (n 16), 108; G. De Anna, 'Automi, responsabilità e diritto' (2019) Rivista di filosofia del diritto 131.

[21] *Business Analytics* can be here summarily defined as the set of tools and software applications for accessing, analyzing and viewing data that helps management quickly grasp the relevant information and control company performance in making the most effective decisions.

[22] De Tullio (n 9), 640.

[23] Ibid., 639 and 650. A possible solution, envisaged to overcome the problem, has been identified in the limitation of the maximum number of variables to be used in Big Data analysis, but the problem of unexpectedly extracted data, as well as additional data, would remain open, even in this hypothesis information obtained thanks to the predictive effectiveness of the algorithms used, F. Casi, 'Big Data ed etica dei dati' (28 December 2018) Consulta di Bioetica Onlus <https://www.consultadibioetica.org/big-data-ed-etica-dei-dati-di-fiorello-casi>.

[24] See, for example, 'Profilazione 2.0: dimmi come clicchi e ti dirò chi sei' (28 September 2010) MyMarketing.net <http://mymarketingnet.blog.kataweb.it/2010/09/28/dimmi-come-clicchi-e-ti-diro-chi-sei/>.

opposition to some policies on data portability.[25] The economic value of Big data is a product of the refinement of knowledge extraction techniques, rather than the amount of data itself.[26] The possibility of collecting, processing and crossing personal information progressively assimilates individuals to sensors in the environment[27] and leads to a redefinition of individual self-determination capable of placing knowledge and the effectiveness of its guarantee at the center of reflection.

3. *Big Data and Privacy*

A significant problem concerns the difficulty in establishing when and to what extent the user is actually aware of the collection of personal data[28] and is free to consent to their processing – considering that access to specific data is not always an indispensable condition for the use of a service, in the light of IT mechanisms, such as tracking walls, which can exclude from a particular service users who refuse to extend the consent provided to it also for another service[29] or who act as marginalizing factors and forcing consent, as happens in the case of devices tracking.[30] The doubts about the freedom in the granting of consent are further intensified if only we consider the current indispensability of some services in interpersonal communications:[31] the apparently free acceptance of users allows companies to exploit personal information, posing serious questions on the protection of confidentiality and freedom of expression, as, in order to "hide", the individual could, as a last resort, renounce the freedom to choose the contents to access and the sites to visit on the Net.[32] In this case, the refusal to provide their information "would imply exclusion from an increasing number of social processes, from access to knowledge to the supply of goods and services",[33] thereby damaging individual and community rights. The protection of privacy appears, in fact, entrusted to an unfair negotiation between entrepreneur and consumer which for the latter is resolved in a mere take or leave,[34] a

---

[25] Orefice (n 8), 62.
[26] G. Della Morte, *Big Data e protezione internazionale dei diritti umani. Regole e conflitti* (Editoriale Scientifica 2019), 161.
[27] Talia (n 2), 81.
[28] Amato Mangiameli (n 16), 112.
[29] A. C. Zanuzzi, 'Internet of things e privacy. Sicurezza e autodeterminazione informativa', in P. Moro and C. Sarra (eds), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica* (Franco Angeli 2017) 115.
[30] Ibid. 116-118.
[31] Consequently, it can be understood that the information for the granting of consent, although compliant with the 2016 Regulation, does not seem sufficiently effective to stem the increasing use of Big Data in the market and their predictive potential, lending themselves to applications mostly formalistic, Delmastro and Nicita (n 11), 142.
[32] Orefice (n 8), 106-107; S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli* (Laterza, 2012) 26.
[33] Ibid. 29. These practices, although widespread, are in contrast with Art. 4 GDPR, concerning informed consent: in fact, a request that includes non-homogeneous purposes or that prevents or disturbs the use of a service offered online is not compliant with the Regulation, as well as with the requirement of the freedom of consent, given that the latter cannot be considered effectively free when its transfer constitutes the price of the service; see Orefice (n 8), 110-111.
[34] On the need to set competition policies using criteria that take privacy into due account and, more generally, on the link between privacy and competition, G. De Minico, 'Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria' (2019) Diritto pubblico 89, 109-113.

situation aggravated by the circumstance that frequently sees the user sign a single contract with the same supplier of services, transferring huge amounts of information into the hands of a single subject,[35] with profound repercussions on individual and collective self-determination of information.[36] In such cases, the withdrawal of consent appears to be an ineffective and hypocritical remedy since it keeps the owner of the information in a subordinate condition, being effectively excluded from an autonomous decision-making power over his own data.[37] In the Internet of Things sector, there is also a concrete risk of involuntary activation of the smart device and unconscious transfer of data, with a clear loss of information control and decision-making power on the user's personal information.[38] It is also necessary to highlight how the evaluation of the freedom and awareness of consent to processing would concern personal data, that is, referable to specific interested parties, while Big Data tends to work on anonymous data: in this regard, it does not seem to be excluded anyway a reason for damage as Big Data, while using anonymous data, after appropriate correlations,[39] become referable to very specific people.[40] In any case, the European legislative framework, while not directly contemplating Big Data,[41] establishes some fundamental principles in the collection and use of personal

[35] Palanza (n 3), 3.

[36] De Tullio (n 9), 665.

[37] Ibid.

[38] Zanuzzi (n 29), 110. It should be remembered the Opinion 8/2014 of WP29 which specifies that, in order to the processing to be considered lawful, users must remain in full control of their data throughout the life cycle of the device. The critical issues mentioned could be referred both to the nature of the device of smart objects as to a lack of coordination between the stakeholders in the processing of personal data, in relation to the adoption of the necessary minimum security measures, see id., 103-106. In the first hypothesis, one could appeal to compliance with the *privacy by design* criterion that is expressed by Art. 25 GDPR, which anticipates the protection of personal data from the planning of the treatment. It should also be mentioned Art. 32 of the Privacy Code which obligates electronic communications service providers to adopt the "technical and organizational measures appropriate to the existing risk to safeguard the security of its services and to comply with the provisions of Art. 32 bis" (i.e. for notifications in the event of data breach). In the same line of guarantee of personal information, Art. 24 GDPR indicates the *accountability* principle, referring to the set of measures that the data controller and the data processor must implement to "guarantee and be able to demonstrate that the processing is carried out in accordance with this regulation". This is a criterion suitable for investing the entirety of company operations, F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679* (Giappichelli 2016), 288. The guarantee of privacy by design and the accountability are accompanied by the respect for *privacy by default*, Art. 25 GDPR, which provides that only the personal data necessary and sufficient for each specific processing purpose and for the period strictly necessary for these purposes are processed by default. On this argument, see Iasselli (n 4), 180-181. Finally, the mentioned criteria are flanked by Recital 78 GDPR which states that "the protection of the rights and freedoms of individuals with regard to the processing of personal data requires the adoption of adequate technical and organizational measures to guarantee compliance with the provisions of this Regulation [...]. Such measures could consist, inter alia, in minimizing the processing of personal data, pseudonymising personal data as soon as possible, offering transparency regarding the functions and processing of personal data, allowing the data subject to control the data processing and allow the data controller to create and improve the security features".

[39] Della Morte (n 26), 161.

[40] De Minico (n 34), 95.

[41] It should be noted that the European Regulation does not make direct mention of Big Data, excluding from consideration data capable of returning information that is sometimes more than sensitive about the individual and capable of profoundly affecting the expression of fundamental rights.

information and, as recent judgments of the Court of Justice of the EU highlight, the need for an effective data protection which should, in principle, prevail over economic interests,[42] considering privacy as an inviolable and essential right both for the formation of the individual personality and for the development of relationships.[43] In this regard, we can only mention here an articulated and exemplary ruling of the German Federal Constitutional Court of 15 December 1983 – with which a real theory on informative self-determination is elaborated – built on the assumption that if on the one hand the individual cannot be exclusive owner of his data – which, representing the social reality, are considered as neutral information – has the right to control over the latter, representing the same a manifestation of the right to the full development of his personality, attributing to the legislator a role of balancing assumptions and contexts that make it possible to limit the right to privacy.[44] Finally, the EDPS, in various opinions and initiatives, did not fail to underline the importance of a consistent regulatory application in the era of Big Data, elaborating the concept of protection of personal information and underlining the need to seize the opportunities offered by new technologies, without allowing them to determine the social values of reference.[45] The challenge to be grasped – and for which the traditional rules and principles that can be deduced from international and national law often appear inadequate and obsolete, suggesting highly deformed systems and technical solutions delegated to private subjects[46] – is to harmonize often conflicting interests and needs, such as transparency and confidentiality of information, data protection and global security,[47] privacy and right to be informed, obtaining an adequate balance between market logic and the essential guarantee of prevailing and non-negotiable rights.[48]

4. *Big Data and Information*

The cooperative and participatory use in the public sphere of some types of Big Data can have a strong social interest, just think of the sharing of information in a smart city, of the monitoring of data aimed at implementing environmental protection and, above all, of the scientific context where the sharing of Big Data opens up to the dispensing of scientific research and its results.[49] In such cases, the information

---

[42] European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement, P8_TA(2017)0076.
[43] De Tullio (n 9), 653.
[44] Cf. Bundesverfassungsgericht, 15.12.1983, 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83; Della Morte (n 26), 166.
[45] European Parliament, Plenary session 2/03/2017.
[46] On the dialectic and the equilibrium of the main "axes of tension" between opposing rights, Della Morte (n 26), 175-227.
[47] For Ziccardi, the debate would concern not so much security as the real possibility of global surveillance, G. Ziccardi, *Il libro digitale dei morti. Memoria, lutto, eternità e oblio nell'era dei social network* (UTET 2017), 88.
[48] Rodotà (n 6), 21 ff. On the link and balance between constitutionally protected values such as freedom of communication, information, and protection of privacy on Web, M. C. De Vivo, 'Comunicare in Internet. Con che diritto?' (2000) Informatica e Diritto 125.
[49] Palanza (n 3), 128.

appears to be declined in favor of knowledge and equality[50] as the foundation of the democratic participation it would like – as recalled by Art. 19 of the Universal Declaration of Human Rights, as well as Art. 21 of the Italian Constitution – free and legally guaranteed access to knowledge and culture.[51] The exploitation of Big Data can be functional both to the enhancement of economic freedoms and to be at the service of inviolable rights and equality.[52] A pressing unknown factor is therefore given by the progressive concentration of information in the hands of a few operators, a phenomenon that is reflected in the full implementation of the rights of freedom and in the future of democracy. The digital platforms, called Over the Top (OTT) or *digital giants*, Big Tech, represent subjects capable of developing services hierarchically above the traditional physical infrastructures of fixed and mobile telecommunications access to the Net and able to assert a intermediation between the sides of the market based on a very high intensity technological structure and based, as regards the use of data, on vertical integration models,[53] giving rise to a marked information polarization.[54] The process of information concentration therefore seems to stand against the principle of substantial equality, which is expressed by the involvement in the cognitive process formed with the contribution of everyone,[55] as well as against the protection of competition and the legal construction of a transparent data-given market[56] that the data collected by the OTTs become the exclusive domain of a few players, able to place barriers to entry to new competitors, distorting the game of competition even in the absence of abuse,[57] to the obvious detriment of the consumer.[58] The ownership of data is then imposed as an essential facility of an intangible nature, indispensable to compete on the market, resulting in the obligation to open data for the information giants,[59] shifting attention from the element of consent to the responsibility of OTTs, in order to reduce phenomena of asymmetric distribution of information resources or undue surveillance by focusing economic processes on fundamental rights.[60] "The masses of data should be at the service of individual growth, equal access for the benefit of other operators and the

---

[50] On the potential of Big Data in the prevention of human rights violations, L. Nosari, 'Potenzialità e problematiche afferenti l'utilizzo dei Big Data in materia di diritti umani' (17 April 2018) CYBERLAWS <https://www.cyberlaws.it/2018/big-data-e-diritti-umani>.

[51] J. Drexl, 'Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of post-truth politics' (2016) Max Plank Institute for Innovation and Competition Research Paper No. 16 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881191>.

[52] De Tullio (n 9), 644.

[53] Delmastro and Nicita (n 11), 51-53.

[54] Ibid. 125.

[55] De Minico (n 34), 113.

[56] Delmastro and Nicita (n 11), 31. The right to the portability of personal data, structured and unstructured, enshrined in Art. 20 GDPR, seems to correspond to this logic, id. 129-130.

[57] De Tullio (n 9), 660. Art. 102 TFEU requires the abuse in addition to market power and a significant price increase, that is, it does not punish market dominance in itself but its misuse to the detriment of consumers and competitors. In any case, any sanctioning measures could not be resolved in mere repressive orders of anticompetitive conduct but should be *privacy based.* On the ways in which the classic remedies of antitrust law could operate in *data driven* digital markets; see De Minico (n 34), 103-109.

[58] Orefice (n 8), 11.

[59] Ibid., 13.

[60] Ibid.

return of data to those who procured them ab initio".[61] In a system inspired by the aims of political, economic and social solidarity, aimed at achieving the full development of the person – Art. 2 Italian Constitution – the data collected by companies should be common goods whose open access, compatibly with privacy needs, subtracts the democratic communication circuit from the self-referentiality of the market.

The ability of online platforms to influence appears equally effective in the political context as they can affect the choices of citizens, even reaching, in some cases distorting, the hierarchical organization, *ranking*, of the news in search, especially in the electoral period. The amount of information available online also corresponds to a greater amount of disinformation strategies based on fake news,[62] so the quality of information ultimately depends on the critical and discerning ability of the end user.[63] In these circumstances, the risk represented by the landowners of knowledge[64] in sending partial messages – frequently selected through the *Sentiment analysis*[65] and with the practice of *clickbaiting* – is evident and it is increate by the use of bait-titles created to attract clicks and arouse viewing of Web pages, capable of affecting the free action of the individual and of questioning the most basic democratic principles.[66] Individual profiling, determined by the application of the appropriate algorithms,[67] thus contributes to selecting crucial content for the formation of public opinion, to be reported to the individual as well as to the political agenda.[68] In the creation of a *filter bubble*, aimed at showing the user the information that the algorithm has calculated for him as potentially interesting,[69] all the asymmetry between the provider of the information service and the user is shown, aggravated by the absence of transparency of the criteria set underlying the functioning of the algorithm.[70] For these reasons, the importance of the *explainability* of the results produced by artificial intelligence

---

[61] De Minico (n 34), 101. Moreover, if we only consider the origin of the information obtained from Big Data, we can well understand how the claiming of exclusive positions is incompatible with the third party ownership with respect to the assets of the claimant, in our case the OTTs, where the only claims operable would seem more like those of a depositary of other people's assets; see id., 90.

[62] Talia (n 2), 13. In this regard, it should be remembered the mental shortcut of the "confirmation bias" for which, in the selection of relevant information, one generally feels more attracted to those that confirm the starting subjective convictions: this breach is inserted into the selection content operated by the algorithm to suggest what could probably arouse interest, based on preferences already expressed. This procedure, as can be seen, establishes a double information filter, determined by the joint action of the algorithmic choice and the confirmation bias, Delmastro and Nicita (n 11), 95-97.

[63] Ibid. 93. The Control Authority for Communications Guarantees has launched a monitoring table on the self-regulation put in place by search engines and social networks, anticipating the work started by the European Commission with the establishment of the *High Level Group on Fake News and Online disinformation*; see id., 135.

[64] Orefice (n 8), 158. The subjects able to carry out an effective concentration of information are represented not only by Google, Facebook or Microsoft, but also by authoritarian governments and government security agencies on anti-terrorist mission: on the numerous legislative initiatives, which multiplied mainly after 11 September 2001 and directed to counter international terrorism; see Palanza (n 3), 14.

[65] Talia (n 2), 101; Orefice (n 8), 25.

[66] Ibid. 158 and 182; Simoncini and Suweis (n 15), 94 ff.

[67] Amato Mangiameli (n 16), 109.

[68] Delmastro and Nicita (n 11), 91.

[69] Amato Mangiameli (n 16),109.

[70] Talia (n 2), 97.

algorithms should be highlighted, in addition to the *knowability* of the automated decision-making process and of the data used in it, especially when they have the task of deciding in a completely automated way, producing legal effects and significantly affecting personal rights and freedoms.[71] The algorithmic logic of the predictive type, which permeates the entire process of extraction, collection and storage of Big Data, is profoundly changing the traditional mechanisms of power by introducing new decision-makers[72] and raising new and pressing questions about possible dangers of algorithmic discrimination of social groups perceived as external to the social fabric and marginalized through self-fulfilling predictions.[73] The predictive analyzes can then have, then, detrimental effects for the subjects involved regardless of the error or inaccuracy of the algorithmic forecast.[74] The central question becomes how to reconcile the regulatory and prescriptive function of law – in particular of international law and of the multiple systems of protection of fundamental rights that are expressed in forms of protection of minorities – with the logic underlying policies based on the capillary collection of information and expression of the direction of prevailing forces.[75] The essential respect for the person, in the dual individual and collective dimensions, necessarily places Big Data in the social context, configuring its use as an asset to be evaluated in relation to the specific purposes of employment.[76] From this direction derives the indispensability of a correct balance with the opposing value of privacy by evaluating whether the means used are suitable, necessary, proportionate to its pursuit:[77] the protection of personal confidentiality appears to prevail over the identification of market models and of typical consumers, in coherent explanation of Articles 41 and 42 of the Italian Constitution aimed at promoting social utility, attributed to private economic initiative, and the social function that belongs to private property.[78] In a different way, the use of Big Data currently seems to endorse economic interests or social control of the State, phenomena that require a strengthening of the guarantees payable by the citizen as well as by the community, first of all in the performance of those automated procedures aimed at take decisions that may affect the exercise of fundamental rights. Once again, all the urgency of an effective regulation of Big Data and, more generally, of personal information circulating online is shown, inspired by constitutionally guaranteed values[79] and based on globally recognized principles of protection of privacy,[80] aimed mainly at protection of the individual from the improper use of information technologies,

---

[71] Palmirani (n 13), 73-92.
[72] Della Morte (n 26), 8.
[73] De Tullio (n 9), 662.
[74] De Minico (n 34), 97. In the treatment of Big Data, this would entail, according to the author, an unavoidable factor of uncertainty, a "forecast risk", falling within the more general business risk, such as to generate, for the author of the algorithm or for the its user, an increase of responsibility, having to respond in the event of a harmful forecast because it discriminates against certain social categories or because it is based on erroneous calculations, regardless of the presence of negligence or willful misconduct, see id., 93-97.
[75] Della Morte (n 26), 9.
[76] De Tullio (n 9), 642.
[77] Ibid., 646.
[78] P. Perlingeri, *Il diritto civile nella legalità costituzionale* (Edizioni Scientifiche Italiane 1991), 444-445.
[79] Simoncini and Suweis (n 15), 103.
[80] Della Morte (n 26), 126.

avoiding any possible deresponsibility attributed to the interpretative capacity of the algorithms used.[81] In perspective, and also in accordance with the provisions of Art. 21 of the Italian Constitution on the freedom of expression of thought, emerges the need to evaluate access to the Internet as a fundamental right of the person and to consider knowledge as a global public good by promoting widespread use of Big Data aimed at attacking substantial inequalities and create the conditions for an authentic self-determination avoiding, except for specific hypotheses envisaged to protect the inviolable rights of the person and the community, any possible phenomenon of information closure, capable of transforming a usable good into a limited resource.[82] This would mark an important step towards shared knowledge and a properly interactive world, inaugurating an effective model of digital citizenship and generating a new form of civil solidarity fueled by information.[83] The realization, through adequate legal guarantees, of balanced social relationships opens up a possible meeting point between productive needs and human needs, in the full respect and in the enhancement of freedom, dignity and diversity of each person, elements that pertain to the intimate constitution of contemporary democracies.[84]

---

[81] Rodotà (n 6), 39. In this regard, see the *Statement on Algorithmic Transparency and Accountability*, 12/01/2017, published by, the US Association of Computational Mechanics (USACM), as well as the European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, P8_TA(2017)0051.

[82] Rodotà (n 6), 72.

[83] Orefice (n 8), 25. In Italy, the Legislative Decree 25 May 2016, No. 97 introduced the so-called generalized access, subject to the citizen's request, followed by any response from the state administration. This procedure, however, turns out to be distant from the Open Data policy and from the full implementation of the principle of transparency, capable of feeding a network of sharing interoperability and reuse of knowledge; see id., 46-73. On the implementation of the open paradigm in the Italian legal system, id., 29 ff. On the most relevant issues concerning Open Data and the reuse of public data, see the monographic issue D. Tiscornia (ed.), *Open Data e riuso dei dati pubblici* (2011) Informatica e Diritto.

[84] S. Rodotà, 'Privacy, libertà, dignità. Discorso conclusivo della Ventiseiesima Conferenza Internazionale sulla protezione dei dati' (2004) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293>.