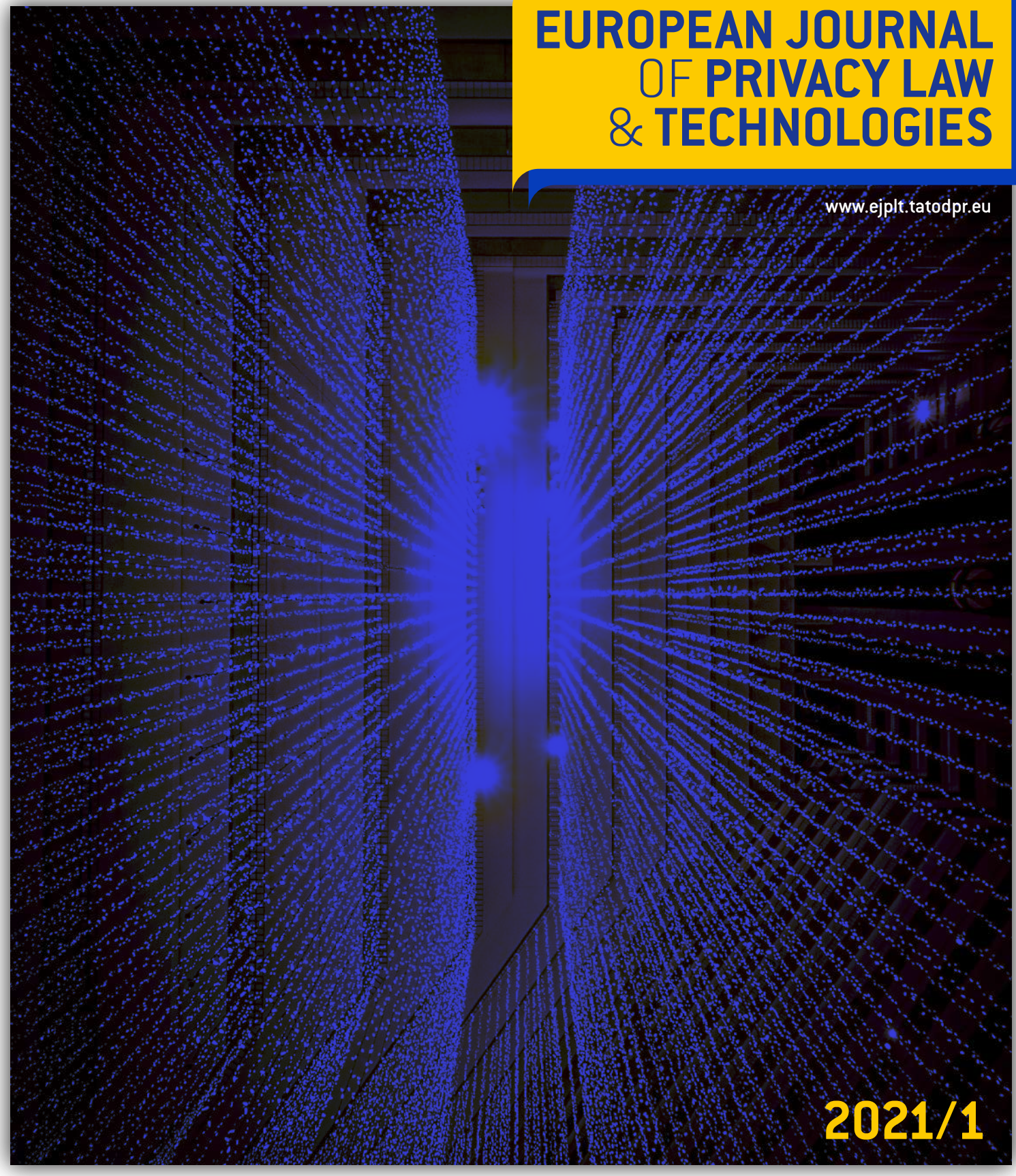
ISSN: 2704-8012

UNIVERSITÀ DEGLI STUDI
SUOR ORSOLA
BENINCASA

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

www.ejplt.tatodpr.eu



2021/1

EJPLT
ISSN: 2704-8012

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

Directed by Lucilla Gatt

2021/1

UNIVERSITÀ DEGLI STUDI
SUOR ORSOLA
BENINCASA

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

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

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

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

Published by Suor Orsola University Press in December 2021
www.ejplt.tatodpr.eu

Editing
Luciana Trama

Design and development
Flavia Soprani, Emanuele Garzia

European Journal of Privacy Law & Technologies

EJPLT
ISSN: 2704-8012

European Journal of Privacy Law & Technologies

EJPLT
ISSN: 2704-8012

pp.

Section I: **Articles**

Section II: **Focus papers**

SECTION I
ARTICLES

EJPLT
European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Digital Markets between Regulation and Competition policy. Converging agendas.

VALERIA FALCE
Full professor of Economic Law, Jean Monnet Professor in EU Innovation Policy, Innovation, Regulation and Competition Policy Centre' Director (ICPC), Università Europea di Roma

The EU data strategy framework is driven by a renewed centralized approach when it comes to regulation. In the following it will be proven that such institutional and governance solution shall not be demonized.
Whereas the European digital culture shall be nurtured and fostered, leading to an a solo, competition law and enforcement shall be maintained fit, strong and fast to as to allow the European sovereignty to stand within and across the national boundaries on one hand, and to expand as a global model, outside the European borders.
To advance such trajectory, competition law and enforcement, both at European level and at national level, shall be kept autonomous and parallel so that to make digital markets contestable and open, while preserving their pro-competitive and pro-innovative functioning.

Keywords: EU Data strategy; Regulation and Competition policy; Digital Markets Act; Digital Service Act.

Summary: Introduction. – 1. A neverending dilemma. – 2. A new innovation policy approach. – 3. Towards a common digital culture. – Conclusions.

Introduction.

On December 15th 2020, the European Commission presented two proposals for the regulation of online platforms. The first concerns the regulation of digital services (hereafter, the "Digital Services Act" or "DSA") while the second constitutes a regulation of digital markets (hereafter, the "Digital Markets Act" or "DMA").

In order to sum up the content of the proposals presented by the European Commission - whose legal basis is, for both of them, the provision set forth in Article 114 TFEU - the DSA addresses the preparation of a specific mechanism for accountability of the platforms for processing and disseminating digital content "uploaded" by users; while the new regime outlined by the DMA envisages a series qualitative criteria aimed at identifying large online platforms having the function of access control (also known as "gatekeeping"). Regarding the role played by gatekeepers, they basically constitute platforms holding consolidated and stable position in the domain of their activities (which could be current or even foreseeable in the near future), hence significantly affecting the internal market and playing an intermediary role between a large base of end-users and a large number of businesses.

Having said that and left aside, for the moment, the "detailed" content of the proposals of the European Commission, it should be noted the DMA and the DSA constitute a "privileged observatory" for investigating the issue of the interdependence between regulation and competition. They should be analysed, on the one hand, under the today's fourth industrial revolution perspective, which involves the "innovative" profile of digital markets; on the other, they should be examined having in mind the "centralized" enforcement undertaken the European Commission and the "national-based" enforcement on the territory of Member States, the latter being upheld by national competitions and/or domestic regulatory authorities.

The inseparable relationship between regulation and competition is neither new nor scantily investigated. As proof of the relevance of the topic – as well as of the temporal "circularity" relationship existing between the two -, in a paper issued few years ago and according to two well-known professors of industrial economics and competition law, i.e. D. Carlton and R. Picker, "*[a]ntitrust can say no but struggles with saying yes […] while regulators often have a hard time saying no*".[1]

[1] D.W. Carlton, R.C. Picker, Antitrust and Regulation, in N.L. Rose (ed.), Economic Regulation and Its Reform: What Have We Learned?, NBER Books, National Bureau of Economic Research, 2014, pp. 25-61.

1. A never ending dilemma.

Under the labour division perspective, the abovementioned reference represents a paramount of the traditional work of conceptualisation - confirmed for decades in both overseas and European manuals[2] - concerning the analysis between antitrust law and regulation. It constitutes a subdivision of such fields, moving transversally into the temporal dimension, that is to say that it moves from an *ex-ante* intervention - in relation to the role of the regulator – to an *ex-post* intervention for antitrust enforcement purposes.

This reading summarises the institutional relationship between regulatory intervention and antitrust law, showing a so "precarious" balance as to have produced a predictable outcome and – it could be said - a state of "permanent conflict", which occurs whenever the enforcement of competition law goes beyond (for the decision purpose or for the methods of "closing" an investigation, e.g., by accepting commitments) the *ex-ante* intervention or, finally, whenever antitrust authority exercises its regulatory powers over the *ex-post* regulatory scenario, by sanctioning certain procedures or settling disputes.

Save for cartels and hard-core restrictions, such a logic "short circuit" reveals itself, on the one hand, in the determination of dominant positions (including those deriving from mergers between companies, on which the power of the competition authority operates through *ex- ante* intervention) and, on the other, in the qualification of market abuses. To this end, the most extreme logic pattern for choosing between antitrust law and regulatory power could be seen in the famous Trinko case,[3] whereby the United States Supreme Court upheld that, in the presence of a sectoral regulation, there is no "division" of labour, but an exclusive prevalence of regulation, also with regard to the governance of *ex-post* conducts.

This having been said, these conceptualisations of the antitrust enforcement and regulatory oversight under the "temporal" subdivision perspective (*ex-ante* intervention vs. *ex-post* intervention) - including the "one-way" reading of the United States Supreme Court Trinko case – present numerous perplexities, especially regarding the presence of market dynamics with a high rate of innovation, such as those which we have been occurred more and more frequently in the last five years.[4]

---

[2] On this topic, see Hovenkamp, Economics and Federal Antitrust Law, St. Paul, West Publishing Co., 1985, p. 9- 10; R.A. Posner, Oligopoly and the Antitrust Laws: A Suggested Approach, 21 Stan. L. Rev. 1562 (1969); P.E. Areeda, Introduction to Antitrust Economics, 52 Antitrust L.J. 523 (1983); G.J. Stigler, A Theory of Oligopoly, in Journal of Political Economy, 72, (1964), 44 ss.; R. Whish, Competition Law, Oxford, OUP, IX ed., 2018, passim; D. Geradin, A. Layne-Farrar, N. Petit, EU Competition Law and Economics, Oxford, OUP, 2012, passim

[3] U.S. Supreme Court, sent. Verizon Communications Inc. V. Law Offices of Curtis V. Trinko, LLP., No. 02-682 (2004).

[4] On this matter, See public consultation, launched on June 26th 2020 and concluded on October 9th 2020, relating to the revision of the EU Commission Communication on the definition of the relevant market for the purposes of applying EU competition law, available at the link: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12325-Evaluation-of-the-Commission-Notice-on-market-definition-in-EU-competition-law. According to the media release on the launch of the public consultation as of June 26th 2020 (available at the link: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1187), "[o]ver the past few years, change is happening at an ever more rapid pace, and the world is becoming increasingly

In this dynamic process of transformation of digital markets, as analysed under the lens of innovation, it is straightforward to acknowledge that both regulation and antitrust law must play their role and, therefore, shall be interpreted as complementary interventions, regardless of the well-known distinction between *ex-ante* and *ex-post* intervention. The regulation sets, on the one hand, the (corrective) purpose of economic freedoms interwoven with "incomplete" rights (to use a terminology employed by the economic analysis of law), hence based on a "given state of the world". Antitrust Law, on the other, regulates the "special" liability arising out from practical situations which cannot be set *a priori* by regulation but, moving from the latter, such practical situations could be subject in re-regulation processes, as long as it is possible to acknowledge every situation as such.

However, as a matter of fact, this means that regulation and competitive enforcement shall be dynamically integrated, which helps, as such, in defining a much broader and a more complex field of investigation in comparison to the mere distinction between *ex-ante* and *ex-post* action.

In light of the above, the DMA and the DSA once again allow this "state of the art" to be critically evaluated and "recorded", outlining the new institutional structure and spending some "embryonic" reflections on the dynamics that will be witnessed over the years to come. Especially, such reflections focus on the necessary interrelationships between regulation and the "traditional" technical-legal tools of antitrust law and, above all, between the "centralized" enforcement system as provided for in the DMA and DSA by the European Commission and those "crumbling" and fragmentating pressures of antitrust enforcement, which have been increasingly put in place by national competition authorities (and which will be discussed below by providing some symbolic examples).

2. A new innovation policy approach.

The proposal provided for in the DMA refrain Member States from imposing on gatekeepers '*further obligations by way of laws, regulations or administrative action for the purpose of ensuring contestable and fair markets*' [5] and '*from applying national rules which are specific to the types of undertakings and services covered by this Regulation* [that is to say, the DMA].'[6] At the same time, the DMA '*is without prejudice to Articles 101 and 102 TFEU, to the corresponding national competition rules and to other national competition rules regarding unilateral*

digital and interconnected. Changes such as the increase in global trade, including with major emerging markets, the progressive elimination of national barriers to commerce within the single market, digitization, and the rise of major new players in some sectors, mean that many markets may work differently today than they did in the past. The current Market Definition Notice dates from 1997 and may therefore not address all pertinent questions arising today when defining the relevant product and geographic market". More recently, the EU Commission issued, on July 12th 2021, a Staff Working Document (SWD(2021) 199 final) reporting an evaluation regarding the update of the EU Commission Communication on the definition of the relevant market for the application of European Law and, especially, in the antitrust field, available at the following link: file:///C:/Users/WIN7/Downloads/090166e5df9d4c7b.pdf.

[5] Art. 1, paragraph 5, Digital Service Act.

[6] Recital no. 9, Digital Service Act.

behaviour that are based on an individualised assessment of market positions.'[7] In details, such a proposal of the European Commission does not '*precludes Member States from imposing obligations, which are compatible with Union law, on undertakings, including providers of core platform services where these obligations are unrelated to the relevant undertakings having a status of gatekeeper*.'[8]

Therefore, any obligation imposed on the "designated" gatekeepers under national competition law is allowed, provided that it is compatible with Regulation (EC) no. 1/2003[9] and, conversely, that '*national authorities shall not take decisions which would run counter to a decision adopted by the Commission',* pursuant to the DMA.'[10] But let's start from the beginning.

Parallel imposition of obligations will therefore be possible, for example, under the DMA and under the new Article 19a of the German Competition Law, which addresses digital platforms.[11] In the case of parallel applications of a regulatory "tool", such as those provided for in the DMA and in competition law, the Court of Justice has previously upheld that, on the one hand, there is a very limited "*room for discretion*" for the European Commission (and, in any case , to be strictly interpreted) to exclude the applicability of Article 102 TFEU, should any anti-competitive behaviour be imposed on companies by national regulatory legislation; and that, on the other, the adoption of *an ex-ante* measures by the national regulatory authority does not preclude the European Commission from launching investigations and/or inquiries pursuant to Article

[7] Ibidem.
[8] See Art. 1, paragraph 5, Digital Service Act.
[9] Pursuant to Art. 3, paragraph 2 of the Council Regulation (EC) No 1/2003 of 16 December 2002, 'Member States shall not under this Regulation be precluded from adopting and applying on their territory stricter national laws which prohibit or sanction unilateral conduct engaged in by undertakings.'
[10] Art. 1, paragraph 7, Digital Service Act.
[11] Art. 19a "Abuse of companies of primary importance for cross-market competition"(1). The Bundeskartellamt may issue a decision declaring that a company that is significantly active on the markets pursuant to Article 18 (3a) is of primary importance for cross-market competition. In determining the primary importance of a company that crosses the markets for competition, the following are taken into account in particular:
1. its dominant position on one or more markets;
2. its financial strength or its access to other resources;
3. its vertical integration and its activities in otherwise related markets;
4. of its access to data relevant to competition;
5. the importance of its activities for third party access to procurement and sales markets and its related influence on the commercial activities of third parties. Once a company is qualified as being of primary importance for cross-market competition, the BKartA may "prohibit this company" from: (2) [...]
1. treat competitors' offers differently from their own offers for access to the offer and sale markets [...];
2. adopt measures that hinder other companies in their activity on the supply or demand markets, when the activity of such companies is relevant for access to these markets [...];
3. directly or indirectly exclude competitors on a market in which the respective firm can rapidly expand its position even without being dominant [...];
4. create or raise barriers to market entry or otherwise foreclose other businesses by using competitive data that has been collected by the other party on a dominated market, including in combination with other competitive data from sources external to the dominated market, or require terms and conditions that allow such use [...];
5. making the interoperability of products or services or data portability impossible or more difficult and therefore hindering competition;
6. insufficiently informing other enterprises of the extent, quality or success of the service they provide or commission, or otherwise making it difficult for them to assess the value of that service;
7. Solicit, for the treatment of offers from another company, advantages that are not proportional to the reason for the request […].

102 TFEU against the same companies to which national measures are addressed.[12] It is not only that, however: the European institutions have interpreted the '*ne bis in idem'* principle very strictly, according to which the same commercial conduct would be sanctioned on the basis of two different regulatory instruments (such as in the case we are dealing therewith, being the DMA and competition rules), provided that the latter guarantees the protection of different legal interests.[13] As, in fact, in the case of the DMA, which aims at protecting a different legal interest, contrary to the rules governing competition: namely, "*it pursues an objective that is complementary to, but different from that of protecting undistorted competition on any given market, as defined in competition law terms, which is to ensure that markets where gatekeepers are present are and remain contestable and fair*".[14] Therefore, the possibility of a joint and parallel enforcement of DMA provisions and competition rules is expressly envisaged.

Conversely, should a "designated" gatekeeper be unable to comply with one set of rules without violating the other, it should then balance itself between the need of preserving and consolidating the internal market (which represents a founding objective as envisaged in the DMA) and, at the same time, respecting the hierarchy of legal sources in European law (pursuant to which European Competition Law - but not also the domestic competition law of the Member States, which goes beyond European law - would prevail over the DMA). Therefore, should antinomies arise out from an obligation imposed by the European Commission pursuant to the DMA (which is applicable throughout the EU) and a measure adopted by a national antitrust authority pursuant to domestic competition law (which is independent from the European law and which applies within one Member State only), the obligation envisaged in the DMA should prevail. Alternatively, it could be argued that, on the basis of the principle of loyal cooperation pursuant to Article 4 TEU, a Member State cannot impose an obligation undermining European law. Should hence a national antitrust authority impose an obligation on a "designated" gatekeeper violating the DMA, the latter could be entitled to refrain from complying with such an obligation, arguing that a Member State would hence impose an obligation in violation to the European law.[15]

In order to "*effectively avoid a fragmentation of the internal market*"[16] and to

[12] See Case C-280 / 08P, Deutsche Telekom, EU: C: 2010: 603, according to which the EU competition rules "complete [...], as a result of an ex-post control exercise, the legislative context adopted by the EU legislator for the ex-ante regulation of telecommunications markets "(§92).
[13] See COMP/39.525, Telekomunikacja Polska, §§143-145.
[14] Recital no. 10, Digital Market Act.
[15] See C-198/01, Consorzio Industrie Fiammiferi (CIF), EU:C:2003:430 Case, according to which: "[…] it is appropriate to point out, first, that, although Articles 81 EC and 82 EC are, in themselves, concerned solely with the conduct of undertakings and not with laws or regulations emanating from Member States, those articles, read in conjunction with Article 10 EC, which lays down a duty to cooperate, none the less require the Member States not to introduce or maintain in force measures, even of a legislative or regulatory nature, which may render ineffective the competition rules applicable to undertakings […] The Court has held in particular that Articles 10 EC and 81 EC are infringed where a Member State requires or favours the adoption of agreements, decisions or concerted practices contrary to Article 81 EC or reinforces their effects, or where it divests its own rules of the character of legislation by delegating to private economic operators responsibility for taking decisions affecting the economic sphere […]" (§§ 45-46).
[16] Recital no. 9, DMA.

"br*ing divergent national legislations closer*",[17] as well as to avoid the risk of different applications of the DMA by the European Commission and of competition law at the level of the States members, the possibility of setting up a new permanent cooperation forum has been proposed (being different from ECN and typical mechanisms envisaged under the Regulation (EC) No. 1/2003, which, contrary to the DMA, fall within the "perimeter" of the "toolbox" available to competition law), whereby the European Commission and national competition authorities (possibly, by virtue of the contribution of other independent national authorities) can meet and discuss the application of the DMA.

Promptly, on June 23rd, 2021, the heads of the national antitrust authorities of the Member States, gathered within the European Competition Network ("ECN"), agreed on a joint document regarding the role of the abovementioned national antitrust authorities in applying the DMA. On the same occasion, the heads of national antitrust authorities supported the creation of a mechanism of close coordination and cooperation between these authorities in the context of DMA, which could emulate the ECN model which has proven to work efficiently over the past 15 years.[18]

3. Towards a common digital culture.

As well-known, the original and fundamental objective of the DMA proposal is to "*allow platforms to unlock their full potential by addressing at EU level the most salient incidences of unfair practices and weak contestability so as to allow end users and business users alike to reap the full benefits of the platform economy and the digital economy at large, in a contestable and fair environment*".[19] But it is not only that, however: the DMA, in the "expectations" of the European Commission's proposal, "*integrates current EU law (and the internal law of the Member States) on competition*".[20]

Doubts about the regulatory fragmentation and the need for harmonization at European level were absent from the "original" purpose upon which the DMA proposal was based. Alongside the start of the legislative procedure, however, certain perplexities emerged prominently, and represent now the core of the debate concerning the adoption of the DMA. And such concerns arise from the circumstance according to which, in order to validly apply Article 114 TFEU as a legal basis, the EU legislator should demonstrate that the real proposal's objective is, indeed, to resolve existing or potential discrepancies between domestic laws being able to hinder the free movement of digital services or restrict competition significantly.

---

[17] Recital no. 8, DMA.

[18] See ECN, Joint paper of the heads of the national competition authorities of the European Union – How national competition agencies can strengthen the DMA (23 June 2021), available at the following link: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Others/DMA_ECN_Paper.pdf?__blob=publicationFile&v=2-.

[19] DMA, Explanatory Memorandum, p. 3.

[20] DMA, Explanatory Memorandum, p. 4, according to which "It addresses unfair practices by gatekeepers that either fall outside the existing EU competition rules, or that cannot be as effectively addressed by these rules. […] The current proposal minimises the detrimental structural effects of unfair practice ex ante, without limiting the ability to intervene ex post under EU and national competition rules".

The Commission proposal moves toward such a direction and warns several times, by general terms, from a risk of probable future regulatory fragmentation. According to the Commission, "*without action at EU level, existing and pending national legislation has the potential to lead to increased regulatory fragmentation of the platform space*".[21]

However, behind the risk of fragmentation that the DMA seeks to avoid, there is a further risk represented by the progressive process of disintegration of the antitrust enforcement going from the "central" level of the European Commission towards the level of the Member States and national competition authorities. It will be possible to enlist some emblematic examples, drawn from the experience of the last year's cases, to openly discuss them, as follows:

- On May 27th, 2021, German, French and Dutch Ministers of Economy and Finance, while welcoming the innovation arising from the DMA proposal, nevertheless requested a greater "*room for domestic discretion*" on the part of Member States to "adjust" to digital markets (and, consequently, apply) specific national competition rules. More specifically, this is how German, French and Dutch governments expressed themselves in the context of this joint statement[22]:

"*National and European legislation should be complementary for addressing issues of market foreclosure and unfairness entailed by the behaviour of digital gatekeepers. These legislations should not undermine each other either. Since the digital economy is complex and multifaceted, a number of constellations may bear national peculiarities. Member States should therefore remain able to set and enforce national rules including national competition law applicable to gatekeepers' unilateral conduct. The framework should grant such national provisions and the enforcement thereof a sufficient and clear leeway, as granted, for example, by the provisions of Article 3 of Council Regulation (EC) No 1/2003 of 16 December 2002*".

- following the German example - whose parliament, as mentioned above, has introduced a specific rule in its competition law, namely the new Article 19a governing the notion of business "*of primary importance for competition and transversal to markets*" - then several other Member States (such as Italy or Sweden) are now considering the opportunity to adopt further national rules inspired by the DMA. And, indeed, the AGCM, in its report to the Government for the purpose of proposing the annual law on competition,[23] has suggested the adoption of Article 3-*bis* of Law no. 287/1990 titled "*Abusive behaviour by companies that are of primary importance for competition on multiple markets*",[24]

---

[21] DMA, Explanatory Memorandum, p. 3; See also DMA, Recitals no. 6-9.

[22] See Germany, French e Netherlands, Strengthening the Digital Markets Act and Its Enforcement, available at the following link: https://www.bmwi.de/Redaktion/DE/Downloads/M-O/non-paper-friends-of-an-effective-digital-markets-act.pdf?__blob=publicationFile&v=4.

[23] S143 – Report as of March 23rd, 2021, pursuant to Articles 21 e 22 of Law 10th October 1990, n. 287, regarding proposals of competition law reforms, pursuant to the Annual Law for Market and Competition on 2021 ('Legge Annuale per il Mercato e la Concorrenza anno 2021'), submitted to the President of the Councils of Ministers.

[24] Article 3-bis. Abusive behaviour by companies that are of primary importance for competition in multiple markets.

1. The Authority, with its own provision being valid for five years from its adoption, can designate companies

by introducing a text modelled on Article 19a GWB.

- The German antitrust authority - the *Bundeskartellamt* - has launched four separate investigations, starting from January 2021, based on the new competition rules approved by the German Parliament with the introduction of the 10th Amendment and of Article 19a to the Competition Law, and, more specifically, the first investigation against Facebook based on the connection of its network with that of the Oculus company on January 28th, 2021,[25] the second against Amazon initiated on May 18th, 2021, [26] the third launched against Google on May 25th 2021 [27] and, most recently, the investigation launched on June 21st 2021 against Apple.[28]

- On May 18th, 2021, the German Federal Court of Justice – *Bundesgerichtshof* - ruled on the appeal of the *Bundeskartellamt* and "overturned", confirming the prohibition, the ruling of the Higher Regional Court of Düsseldorf concerning the clauses of equal price or the "Most Favoured Nation clause" or "MFN

---

that have, in particular, the following characteristics of primary importance for competition in several markets: i) possession of a dominant position in one or more markets; ii) the degree of vertical integration and / or presence on contiguous markets; iii) access to data relevant to competition; iv) the importance of the activities carried out to allow third-party companies to access supply or outlet markets and v) the influence on the economic activity of third-party companies.
2. In the event of an assessment pursuant to paragraph 1, the Authority may, with the same provision, prohibit the designated company from the following conduct, unless the designated company demonstrates that the same are objectively justified:
a) to grant preferential treatment, in the intermediation of access to supply or outlet markets, to its goods or services with respect to those of other companies, in particular by favouring them in the visualization or pre-installing their services or products or by integrating them into other offers of the company;
b) hinder other companies in their economic activities on supply or outlet markets, when the activities of the designated company are relevant for access to these markets;
c) hinder other companies on markets in which the designated company, even without being dominant, could rapidly expand its position, in particular through matched bidding and binding strategies;
d) strategically use the processing of data relevant to competition in order to raise the barriers to entry for other companies;
e) hinder the interoperability of goods or services or data portability;
f) provide other companies with insufficient information on the services provided by the designated company or hinder their ability to evaluate such services;
g) to request conditions for the processing of offers from another undertaking that are not proportionate to the service offered, in particular by requesting the transfer of data or rights not necessary for the provision of the service or by making the quality of the offer subject to the transfer of data or rights that are not proportionate to the service.

[25] See Press release del January 28th 2021 titled: First proceeding based on new rules for digital companies – Bundeskartellamt also assesses new Section 19a GWB in its Facebook/Oculus case , available at the following link: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/28_01_2021_Facebook_Oculus.html?nn=3599398.

[26] See Press release as of May 18th 2021 titled: Proceedings against Amazon based on new rules for large digital companies (Section 19a GWB), available at the following link: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/18_05_2021_Amazon_19a.html?nn=3599398.

[27] See Press release a of May 25th 2021 titled: Proceeding against Google based on new rules for large digital players (Section 19a GWB) – Bundeskartellamt examines Google's significance for competition across markets and its data processing terms, available at the following: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/25_05_2021_Google_19a.html?nn=3599398.

[28] See Press release as of June 21st 2021 titled: Proceeding against Apple based on new rules for large digital companies (Section 19a(1) GWB) – Bundeskartellamt examines Apple's significance for competition across markets, available at the following link: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2021/21_06_2021_Apple.html?nn=3599398.

clause" in the case of Booking.com.[29] Although the case described above constitutes a conduct previously "scrutinized" and authorized by the competition authorities in other jurisdictions of the European Union, and despite the risk of divergent interpretations of EU law, this is a case whereby the European Commission had not intervened and the *Bundesgerichtshof* opted not to submit a preliminary reference to the Court of Justice.

- On July 17th, 2019, the European Commission launched an investigation to assess whether Amazon's use of sensitive data of independent retailers operating on its marketplace has breached EU competition law[30] and, on November 10th, 2020, the European Commission communicated a Notice of Charges[31] to Amazon, also leading, *inter alia*, the investigation to focusing on the European Economic Area excluding Italy, since the AGCM had initiated an analogous investigation concerning similar assumptions and behaviours (with particular focus on the Italian market, anyway) on April 10th 2019,[32] hence allowing parallel proceedings at EU and domestic level in relation to the same conducts.

- On October 7th, 2020, the Polish antitrust authority imposed the highest pecuniary sanction ever applied under competition law (equal to Euro 6.7 billion against Gazprom),[33] in the absence of any communication channel with the European Commission concerning preliminary findings and the purpose to proceeding with such a high penalty, as explained by the EU Commissioner Vestager.[34]

Conclusions.

Coming to some preliminary sharp conclusions it seems that in the new innovation policy agenda, institutional and governance centralization shall not be demonized. Shall be better complemented instead.

Whereas the European digital culture shall be nurtured and fostered, leading to an *a solo*, competition law and enforcement shall be maintained fit, strong and fast to as to allow the European sovereignty to stand within and across the national boundaries on one hand, and to expand as a global model, outside the European borders.

To advance such trajectory, competition law and enforcement, both at European level and at national level, shall be kept autonomous and parallel so that to make digital markets contestable and open, while preserving their pro-competitive and pro-innovative functioning.

---

[29] See Bundesgerichtshof bestätigt Unzulässigkeit der "engen Bestpreisklauseln" von Booking.com, Nr. 099/2021, Beschluss vom 18. Mai 2021 – KVR 54/20, available at the following link: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2021/2021099.html.

[30] See Press Release Release of European Commission, Case AT.40462 Amazon Marketplace, available at the following link: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291.

[31] See Press Release of European Commission, available at the following link: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077.

[32] V. A528 – FBA Amazon.

[33] See Press Release UOKiK, available at the following link: https://www.uokik.gov.pl/news.php?news_id=16818.

[34] See https://www.politico.eu/article/poland-hits-gazprom-with-world-largest-competition-fine/.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

What are digital platforms? An overview of definitions, typologies, economics, and legal challenges arising from the platform economy in EU.

ERION MURATI
Ph.D. Candidate and Lecturer at the Law Faculty
of the University of Hamburg

Abstract

Digitalisation is defining new eras for various economic sectors and human activities. It consists of all interventions to bring what is analogue in the digital dimension. Digitalization sector is the main enabler of the platform economy, which takes the form of the creation of a data (or digital) layer on top of the physical world, providing a parallel virtual map of the world. Digitalisation, embodied by digital platforms, brings efficiency by reducing information asymmetry, transaction costs, search costs, and by empowering new services or large scale of coordinated networks. However, digital platforms raise new regulatory challenges such as, for instance, the need for open data, ensuring a balanced relationship between the platforms and their users, inappropriate existing legal framework for new services, etc. In this light, this paper aims to provide a comprehensive introduction in the dimension of digital platforms by analysing their definitions, typologies, economics, and legal challenges arising from the platform economy in EU. Thus, it provides an examination of the intersection between digital platforms, economics, and law.

Keywords: Digitalisation; digital platforms; data; collaborative economy; legal challenges.

Introduction.

The application layer of the internet is increasingly dominated by the Over-the-Top Operators (OTT), namely online platforms such as Google, Amazon, and Facebook.[1] The ongoing digitization of all aspects of business and life gives rise to so-called online platforms. They play an increasingly important role in today's economy by serving as intermediaries between consumers and suppliers. They provide digital infrastructures, collect, assess, facilitate information exchange, aggregate supply and demand, provide trust, etc.[2] Following the path of companies such Apple and Amazon, more and more firms are trying to become not just product purveyors but also platform provider, facilitating direct connection between customers and other groups. Products produce[3] a single revenue stream, while platforms can generate many.[4] Economists have generally referred to some of them as "multisided platforms" which create value by bringing two or more different types of economic agents together and facilitating interactions between them that make all agents

[1] Telecom operators use also to call them as the OTTs, the Over-the-Top operators, which rely on their infrastructure to generate value.

[2] See section 3. in Murati E, *What are digital platforms? An overview of definitions, typologies, economics, and legal challenges arising from the platform economy in EU*, in EJPLT, Issue. 1/2021.

[3] In a product business model, firms create value by developing differentiated products for specific customer needs, and they capture value by charging money for those items.

[4] In a platform business model, firms create value primarily by connecting users and third parties, and they capture value by charging fees for access to the platform. Platform models bring a shift in emphasis—from meeting specific customer needs to encouraging mass-market adoption in order to maximize the number of interactions and benefit from network effects. Whether or not the leap from product to platform works is an immensely important question. The appeal of such a move is understandable. Products produce a single revenue stream, while platforms—which we define as intermediaries that connect two or more distinct groups of users and enable their direct interaction—can generate many. Indeed, a large number of the world's most valuable companies by market capitalization in 2015 were platform companies, including five of the top 10 (Apple, Microsoft, Google, Amazon, and Facebook). Although some of those companies started with platforms, many started with products: Amazon launched as a retailer in 1994 and six years later introduced Amazon Marketplace; Google began with a search engine in the mid-1990s and then introduced search advertising in 2000; and Apple created the iPod in 2001 but didn't move toward a platform until it developed the iTunes Store in 2003 and the App Store in 2008. In these terms, see Feng Zhu and Nathan Furr (April 2016). 'Products to Platforms: Making the Leap' available at https://hbr.org/2016/04/products-to-platforms-making-the-leap accessed 22 May 2020.

better off.[5] Likewise, the European Commission[6] has clarified that digital platforms operates in two (or multi)-sided markets,[7] they benefit from 'network effects' and they play a key role as organisers of new markets by facilitating new business ventures.

Digitalization sector is the main enabler of online platforms, which takes the form of the creation of a data layer on top of the physical world. Sensors extract data from the physical world (from computers, from smartphones, from Internet of Things sensors, etc.) and a parallel virtual map of the world is constructed. Artificial intelligence (AI) makes it possible to automate the management of the large amount of data extracted from reality.[8] They concentrate the data extracted from the physical word, they have AI capabilities to manage such data and to extract value from it, and they are in the position to create and curate new multi-sided markets and to make new network effects possible. Platforms create new market opportunities, by bringing new entrants and enrolling a 'new workforce' (the car driver, the house owner, etc.) or mobilizing 'new' capital often has a disruptive effect on existing markets and operators, be it the tax companies, the hotels, the financial institutions, the traditional distributor of goods or content.[9] In essence, their business model consists of facilitating interaction between different user groups (be it buyers and sellers, or potential customers and advertisers). They are, therefore, said to operate in multisided markets, where every user group represents a 'side'.[10]

Centralization within the physical and application (or platform) layer can make the operators 'choke points' or 'bottlenecks', where online access can easily be closed down. Accordingly, there is a risk that platforms—like ISPs—start acting like monopolists in their respective layers, e.g., by abusing their market power to exclude competitors or exploit consumers. There is thus a growing consensus that some form of regulation is required to keep the internet open and competitive.[11] Indeed, disruption has become a buzzword to designate this new phenomenon. It has an economic meaning when it refers to the challenge new online platforms present for incumbents. But the term 'disruptions' is also associated with the challenge those entrants pose to the

[5] See David S. Evans Richard Schmalensee (2014) 'The antitrust analysis of multi-sided platform businesses', in Roger d. Blair and D. Daniel Sokol, *The Oxford handbook of international Antitrust economics* (Oxford Press) p. 405

[6] Communication of the European Commission, Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe COM (2016) 288 final, 2.

[7] 'Online platform' refers to a business model operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users in order to generate value for all of the groups. In these terms see, EU Commission (2015) Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, http://ec.europa.eu/digital-agenda/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud [24-11-2015]

[8] Montero J.J, 2019, Regulating Transport Platforms: The Case of Carpooling in Europe, p. 2, in Finger M. & Audoin M, 2019, *The Governance of Smart Transportation Systems*, Springer International Publishing

[9] See Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? p.4 in Bram Deveolder (ed) 'The Platform economy unravelling the legal status of online intermediaries' (Intersentia 2018)

[10] Jean-Charles Rochet and Jean Tirole, 'Platform competition in two-sided markets' (2003) 1 Journal of the European Economic Association 990.

[11] See Bostoen F, 'Regulating online platforms lessons from 100 years of telecommunications regulation, p. 3, working paper.

existing law. Indeed, digital platforms generate many legal disputes, especially when they operate at the margin of existing laws (i.e., labour law in the case of Uber, copyright law, competition and data in the case Google/Alphabet, data protection in the case of Facebook, etc.) Three of the high-profile cases before the European Court of Justice (ECJ) are about the liability regime (or legal status) that applies to *Uber Spain (2017)*, *Airbnb Ireland (2019)*[12] and *Star Taxi App (2020).*

Acknowledging the state of affairs described above, the main aim of this paper is to broadly assess the main characteristics of online platforms (Section 2) and to articulate some views on the economics of digital platforms (Section 3). Among the categories of various digital platforms, we further explore the rise of the collaborative economy in the EU internal market.

This choice is mainly justified due to the legal challenges arsing from it which have been already, somehow, addressed from the ECJ (Section 5.1). However, it is important to underline from the outset that each category of digital platforms (Section 2.1) pones its specific legal challenges in relation to its the market operation (i.e., music, news, app stores, streaming, food delivery, transport, accommodation, etc). In this light, section 5.2 analyses, additionally, the attempt of EU and national regulators to provide a legal framework for digital platforms. Finally, this research has been conducted mainly under the perspective of the business to platform relationship (P2B). The consumer to platform relationship (C2P) is also worth of interests both in terms of recent legal case developments regarding data protection, consumer protection, hate speech, fake news, etc, and the EU goal to enhance consumer protection through the "New Deal for Consumers" initiative aimed at strengthening enforcement of EU consumer law in light of a growing risk of EU-wide infringements.[13]

1. Defining online intermediaries.

The diversity of online platforms in terms of activity, sector, business model, and size are striking. Platforms range from small websites with a local reach to worldwide companies generating billions of revenues. They offer varied services such as Internet search engines (Google, Yahoo), online marketplaces (eBay, Booking, Amazon), video-sharing platforms (e.g., YouTube), music and video platforms (e.g., Spotify, Netflix), social networks (e.g., Facebook, Twitter), collaborative economy platforms (Airbnb, Uber, BlaBlaCar, Ulule, Crowdcube), online gaming (Steam), etc. Finding a common definition for all of them is quit challenging. Several legal definitions of digital platforms have been proposed or even codified in the law. Internet intermediaries has been defined by the Organization for Economic Co-operation and Development (OECD) as entities that "bring together or facilitate transactions between third

[12] See Murati E, (September 2020), *Airbnb and Uber: two sides of the same coin* (September 2020) available at: http://www.medialaws.eu/airbnb-and-uber-two-sides-of-the-same-coin/ accessed 20 October 2020.
[13] Accordingly, was adopted the new Directive on better enforcement and modernisation of EU consumer protection by the European Parliament and the Council on 27 November 2019. See Review of EU consumer law - New Deal for Consumers https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en

parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties". [14] Nowadays, the notion of "intermediary" is increasingly replaced in common parlance by the more palatable term of "platform" which evokes a role that goes beyond one of mere messenger or connector, and extends to the provision of a shared space defined by the applications within which users can carry out their activities and generate value.[15]

Academics argue that platform economy requires a workable definition.[16] It should be affirmed at the outset that there is no general understanding of what an online platform is, especially since it can cover a great variety of different and unrelated fields. The Communication from EU Commission on online platforms[17] is instructive in this respect, insofar as it refrains from offering legally sound definitions. Instead, it lists some common features: a) they have the ability to create and shape new markets, to challenge traditional ones, and to organise new forms of participation or conducting business based on collecting, processing, and editing large amounts of data; b) they operate in multi-sided markets, but with varying degrees of control over direct interactions between groups of users; c) they benefit from 'network effects', where, broadly speaking, the value of the service increases with the number of users; c) they often rely on information and communications technologies to reach their users, instantly and effortlessly; d) they play a key role in digital value creation, notably by capturing significant value (including through data accumulation), facilitating new business ventures, and creating new strategic dependencies."

Accordingly, considering those elements, at least two opposite schemes can be identified.[18] On one side, digital platforms can embody an extremely passive attitude, thereby limiting themselves to behave in a non-interventionist manner and acting solely as a mere virtual (non) marketplace for the match between demand and supply, as in the early days of couch-surfing or in the more modern car-pooling of BlaBlaCar. On the other, digital platforms can be highly engaged, thereby influencing not only the performances of their providers but also the relation they establish with users. For instance, through a complex algorithm, Uber is able to push drivers towards more profitable zones, e.g., shopping centres, railway stations, touristic areas, and to impose differentiated fares during peak time; this practice is known as surging. However, this scheme is fluid too because platforms has always the capacity and the flexibility to change their conditions in any given time as a reaction to

[14] See OECD (2010) *The economic and social role of Internet intermediaries p. 9,* https://www.oecd.org/internet/ieconomy/44949023.pdf Accessed June 2020

[15] Belli L, Erdso D., (2017) "*Platform regulations: how platforms are regulated and how they regulate us*", p. 27, http://bibliotecadigital.fgv.br/dspace/handle/10438/19402 Accessed May 2019

[16] See Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? p. 13, in Bram Deveolder (ed) 'The Platform economy unravelling the legal status of online intermediaries', (Intersentia 2018)

[17] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe, COM (2016) 0288 final,

[18] See Inglese M, *Regulating the Collaborative Economy in the European Union Digital Single Market,* p.12 (Springer 2019)

external factors. For example, recently the Californian legislators approved a landmark bill that requires companies like Uber and Lyft to treat contract workers as employees, if a company exerts control over how they perform their tasks or if their work is part of a company's regular business.[19] Accordingly, and in order to avoid compliance with the new law, Uber is giving drivers now more control over their rides and making fares more transparent — which could mean passengers find that some types of trips get rejected more frequently.[20]

Digital platforms have been defined either broadly or narrowly. A broad definition has been proposed by German Monopolies Commission according to which "platforms are all Internet business providing direct interaction between two or more distinct groups of users that are connected by indirect network effects".[21] Later on, the White Paper on Digital Platforms published in March 2017 by the German Ministry of Economic Affairs and Energy defines platforms as "internet-based forums for digital interaction and transaction".[22] Similarly the French Conseil National du Numérique (CNNum) defines a platform as "a service that provides an intermediary function in the access of information, goods or services that are usually provided by third parties".[23]

On the other side, a paradigmatic example of a narrow definition is to be found in Art. 2 of Discussion Draft of a Directive on Online Intermediaries Platforms, according to which digital platforms "means an information society service accessible through the internet or by similar digital means which enables customers to conclude contracts with suppliers of goods, services or digital content. This does not include services which only identify relevant suppliers and which direct customers to those suppliers' websites or contact details".[24] Likewise the European Commission has defined online platform as "an undertaking operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups. Certain platforms also qualify as Intermediary service providers."[25] The later definition had been criticized as far as that there are firms with a technical basis for delivering content to end users that are not multi-sided but that can

19 See Kate Conger and Noam Scheiber (Sept. 11, 2019) California Bill Makes App-Based Companies Treat Workers as *Employees,* https://www.nytimes.com/2019/09/11/technology/california-gig-economy-bill.html accessed 21 January 2020

20 See Carolin Sayd (Jan. 8, 2020) *Uber makes major changes to California rides as gig-work law takes effect*, https://www.sfchronicle.com/business/article/Uber-makes-major-changes-to-California-rides-as-14957326.php accessed 21 January 2020

21 BKartA, B6-113/15, Working Paper – *The Market Power of Platforms and Networks*, June 2016, p. 2

22 White Paper on Digital Platforms, (2017). *Digital regulatory policy for growth, innovation, competition and participation,* https://www.bmwi.de/Redaktion/EN/Publikationen/white-paper.html Accessed August 2019, pg.21.

23 According to a 2015 report of the French Conseil National du Numérique, Ambition numérique, Pour une politique française européenne de la transition numérique, (June 2015) p. 49.

24 The Discussion Draft of a Directive on Online Intermediary Platforms has been elaborated by the Research Group on the Law of Digital Services, a European network of legal scholars initiated by a group of researchers from the University of Osnabrück (Germany) and the Jagiellonian University Krakow (Poland). See, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2821590 *Research Group on the Law of Digital Services, Discussion Draft of a Directive on Online Intermediary Platforms, 5 (2016) Journal of European Consumer and Market Law 164-169 (Publishers: C.H.Beck, Nomos and Wolters Kluwer)*

25 European Commission, "The regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy" (September 2015) p 4, accessed online https://ec.europa.eu/information_society/newsroom/image/document/2016-7/efads_13917.pdf Accessed 10 January 2020. Accessed 10 January 2020.;

nevertheless be considered to be digital platforms, for example, Netflix.[26]

There are two specific examples of legal codification of online platforms definition. The first one is provided by the French Consumer Code (law[27] of 7 October 2016 on 'La Republique numerique') which uses a broad and dual definition of the operator of platforms. Articles L111-7 and L111-7-2 of the French Consumer apply to 'platform operators', which are defined as "any natural or legal person offering on a professional basis, on a monetary or non-monetary basis, an online communication service to the public based on: 1) the classification or referencing (listing or ranking), by means of computer algorithms, of contents, goods or services proposed or put online by third parties; or 2) The connection of several parties in order to sell a good, provide a service or exchange or share a content, a good or a service

It is interesting to see that the law opts for a platform definition based on its core functions, namely search and matching.[28] The first type of activity of may refer to two sub-types of activities: a) services provided to platform users that identify relevant suppliers and direct customers to those suppliers' websites or contact details (search engines); and b) services of a comparative nature provided to platform users to identify relevant suppliers, customers of other users (comparators). Otherwise, the second type of activity is about different types of intermediation. Since Article L. 111-7 of the Consumer Code uses the words "*mise en relation*", which translates into English as «connection", the platform can be seen as an intermediary, a representative, an agent or a broker.[29] Due to the reference to these two types of activities (infomediary and intermediary), the online platform definition is very broad and for that had been criticized as it risk encompassing too many situations where an intermediary intervenes, including in the old, non-digital economy.[30] However, the legislative choice of a broad definition in the new Article L.111-7 of the Consumer Code can be explained by the fact this new article imposes on platform operators only duties of trustworthiness and duties to inform consumers and other users of online platforms, but not other types of duties or liabilities. Moreover, the new articles of the French Consumer Code leave in

[26] Moreover, firms can make the strategic decision to move from a one-sided to a multi-sided platform and vice versa. See Pieter Nooren et al. "Should We Regulate Digital Platforms? A New Framework for Evaluating Policy Options" in Policy & Internet (2018) p. 267

[27] *Est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur: 1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers: 2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service.* (Art. L. 111-7. – I *Code de la consummation);* LOI n° 2016-1321 du 7 Octobre 2016 pour une République numérique, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id accessed 10 January 2020

[28] Further, the law obliges the online platform operator to offer the consumer faithful, clear and transparent information, especially regarding: a) the general terms and conditions of use of the intermediation service, and the methods of listing and ranking and delisting; b) the existence of a contractual relationship, a capitalistic link or direct remuneration that influences the listing or ranking. In other words, what the law imposes is transparency. On 29 September 2017, three decrees were adopted to specify these obligations. See Bostoen F, "Neutrality, fairness or freedom? Principles for platform regulation" in IPR 2018 V.7 (1), p. 10

[29] See Juliette Sénéchal "Online Platforms under French Law" in U Blaurock (eds) *Plattformen* (Nomos 2018) p. 122

[30] See Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? p. 12 in Bram Deveolder (ed) 'The Platform economy unravelling the legal status of online intermediaries', (Intersentia 2018)

the shade the second facet of online platform operators, who sometimes have a very active role in the context of a relationship between a supplier and a customer.[31]

The second one is giving by the recent EU Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services, also known as Business to Platform regulation (B2P). According to Art. 2 (2) online intermediation services means services which meet all of the following requirements: (a) they constitute information society services within the meaning of Article 1(1)(b) of Directive (EU) No 2015/1535 of the European Parliament and of the Council; (b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users on the basis of contractual relationships between, on the one hand, the provider of those services and, on the other hand, both those business users and the consumers to which those business users offer goods or services;

The provisions of this Regulation aim to address the dependency of many companies on certain online intermediaries' services and their exposure to potentially harmful practices such as unexplained change of terms and conditions without prior notice, delisting of goods and service, lack of transparency relating to the ranking of services, unclear conditions for access to, and use of, data collected by platforms. This definition aligns with EU Agenda aims on the collaborative economy, which does not indulge in defining the concept of online platforms as such. By contrast, it stipulates that, if they provide a service for remuneration, at a distance, by electronic means and upon individuals' request, according to the definition contained in Article 1(1) (a) of the Information Society Services Directive, they fall within the scope of application of the e-Commerce Directive. [32] Almost all online platform self-considers themselves as an information society because of the benefits offered by the E-Commerce Directive. However, the self-declaration is not enough for

[31] The Consumer Code consequently regulates platforms as regulators of two-sided markets, i.e. more as new intermediary bodies between the State and the public, than as intermediaries between two particular economic actors. This conceptual choice is supported by the system applied to platforms not only in Articles L. 111-7, II., L.111-7-1 and L.111-7-2, but also in the proposals of decrees implementing these articles and notified to the European Commission. As a result, the new French rules applicable to platforms can be seen more as a list of positive duties to inform, imposed on these new delegated "regulators", than as a list of pre-contractual bad practices (unfair commercial practices) or contractual bad practices (liability), which would be prohibited. Indeed, the duties to inform imposed on platform operators are a kind of duty of transparency concerning the functioning of the platform for the benefit of the public. This duty can be understood as a counterpart of the delegation given by the French State to the online platform operators to regulate two-sided or multi-sided markets. Moreover, there is neither explicit nor implicit articulation between the new Article L.111-7 and the pre-existing articles of the Consumer Code dedicated to unfair commercial practices or to liability. No more there is an articulation be- tween Article L. 111-7 of the Consumer Code and the Articles of the French Civil Code devoted to the formation and non-performance of con- tract. Article L.111-7 is complemented by a modular service-based approach in Article L.111-7-2 of the French Consumer Code, which is related to the nature of the services provided by the platform operator. In addition to the broad definition of the previous article (search engine, comparator and/or intermediary), Article L.111-7-2 also regulates the online review system provided by websites. See Juliette Sénéchal "Online Platforms under French Law" in U Blaurock (eds) *Plattformen* (Nomos 2018) p. 120.

[32] See European Commission, 'A European agenda for the collaborative economy', COM (2016) 356 final.

reducing the role of the platform to merely intermediary. Therefore, considering Uber, Airbnb and the Star Taxi App rulings of ECJ on unrevealing their real legal status, perhaps is more appropriate to define online platforms as 'open infrastructure[s]' [33] exercising, depending on their mode of functioning, a mere facilitator role or exerting a high level of control and influence over providers and users.[34]

In a nutshell, it is important to consider the economic effects and the business model flexibility of platforms in order to provide a case specific definition of a given platform. Yet, their definition is as dynamic as the possibilities for tech companies to reinvent their business models in the digital economy.

1.1. Typologies of digital platforms.

While it is difficult to describe what platforms *are*, it is easier to describe what they *do*. Thus, to differentiate platforms, first, is suggested to focus on the item/service to which the platform offers access. The for-profit (versus social, cooperative, community-centred) objective is a pre-requisite for avoiding confusion within the 'collaborative economy'.[35] Second, the degree of control of the platform on the underlying transaction is also an important factor to identify the platforms of the collaborative economy from other commercial intermediaries offering a merely intermediation service (i.e., Google Search) or offering, in addition, an offline service (i.e., Uber). Third, it is also worth to make distinction according to the type of operators, whether they operate as business (B) or consumers (C).

One of the first and more comprehensive classification of online platforms has been offered by the OECD which uses six categories based on the kind of services consumers may use through online platforms: i) Internet access intermediaries, ii) hosting and data processing providers; iii) online e-commerce intermediaries; iv) search engines, v) portals; and vi) participative networked platforms. [36] The logic of this classification was also confirmed in EDRi's response to the European Commission's public consultation on online platforms in June 2015,[37] which stated that "it is not useful to have Airbnb, Google News and YouTube categorised as being the same type of business". Considering this, digital platforms have been categorized as it follows. (1) Digital platforms may be divided, depending on their primary function, in innovation and transaction platforms. The former consists of common technological building blocks that the owner and ecosystem partners can share to create new complementary products and services, such as smartphone apps

[33] See G. Smorto (2017) 'Critical assessment of European agenda for the collaborative economy. In depth analysis for the IMCO Committee' IP/A/IMCO/2016-10, PE 595.361, 13-14.; See also M Inglese, *Regulating the Collaborative Economy in the European Union Digital Single Market,* p.15 (Springer 2019)

[35] See Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? p. 11, in Bram Deveolder (ed) 'The Platform economy unravelling the legal status of online intermediaries', (Intersentia 2018)

[36] See OECD (2010), 'The economic and social role of Internet intermediaries', April p. 9, https://www.oecd.org/internet/ieconomy/44949023.pdf accessed 19 February 2020.

[37] See EDRI's answering guide to the European Commission's platform consultation, available at https://edri.org/files/platforms.html accessed 3 February 2020.

or digital content such as from Apple iTunes or Netflix. On the other hand, transaction platforms are largely intermediaries or online marketplaces that make it possible for people and organizations to share information or to buy, sell, or access a variety of goods and services. The more participants, functions, and digital content or services available through a transaction platform, the more useful it becomes.[38]

(2)A second classification[39] of platforms (P) is based on the relationship with consumer (C) or businesses (B) and based on the transactional nature of the relationship, namely: a) Transaction based platform to consumer (P2C) platforms, such as Netflix or Spotify. These platforms utilise content licensed by right holders to platforms. Transactions (subscription) occur on the various sides of the platform, *i.e.,* between platform and right holders and between platform and its users; b) Non transaction based P2C platforms, such as Google news and other news aggregators or review services like Yelp. In these platforms, content is freely available online, with no P2B transaction. Hence, there is no transaction on either side of platform and advertisement is the main business model; c) Zero consumer value P2B services, such as promoted content on social media companies like Twitter. Here the transaction happens on the business side of platforms; d) Transaction based consumer or business to consumer (C2C & B2C) platforms. Examples of this type of platform include companies like Ebay, AirBnB and Uber. Here transactions (fee) take place between businesses and the platform, and between consumers and businesses (B2P & C2B transactions); e) Non-transaction-based consumer to consumer (C2C) platforms. These include UGC, blogging, micro-blogging; In view of this, it emerges that online platform operate in a wide range of market activities.[40]

TYPE OF PLATFORMS	MAIN BUSINESS MODEL	EXAMPLE
Online marketplaces	Transaction fee	Amazon, eBay, Allegro, Booking.com
Collaborative or sharing economy platforms	Transaction fee	Uber, Airbnb, Taskrabbit, BlablaCar, *MaaS* (emphasis added)
Communication platforms	Advertisement, subscription	Skype, Whatsapp, Tinder
Social networks	Advertisement,	Facebook, LinkedIn,

[38] It is mostly the digital technology and scale that make these platforms unique and powerful in today's world. Google Search, Amazon Marketplace, the Facebook Social Network, Twitter, and Tencent's WeChat are examples of transaction platforms used by billions of people every day. Credit cards such as Mastercard, Visa, and American Express, as well as catalogues such as the Yellow Pages (think of this directory as bundled with the telephone), are transaction platforms that originated before the digital era. See Michael A. Cusumano et al, *The Business of Platform. Strategy in the Age of Digital Competition, Innovation and Power*. Harper Business, 2019, p. 55-57.

[39] Ibid.; See also Joe. Mc, & Maryant F.P, (2017) *Fundamental Rights and Digital Platforms in the European Union: a Suggested Way Forward* in *Platform regulations: how platforms are regulated and how they regulate us*". The book is freely available at http://bibliotecadigital.fgv.br/dspace/handle/10438/19402) pg. 100 ss. See also, Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? Cit. p. 9; Paul-jasper D, *Online platforms and how to regulate them: an eu overview*, policy paper no.227 14 june 2018, in Jacques Dolers Institute Berlin.; See Oxera, "Benefits of online platforms. Prepared for Google", October 2015, p. 16-19, https://www.oxera.com/wp-content/uploads/2018/07/The-benefits-of-online-platforms-main-findings-October-2015.pdf.pdf accessed 19 February 2020

[40] See Paul-jasper D, "Online platforms and how to regulate them: an EU overview" policy paper no. 227 14 June 2018, in Jacques Dolers Institute Berlin. p. 4

	subscription	Twitter
Search engines and specialised search tools	Advertisement	Google search, TripAdvisor
News aggregator	Advertisement	Google Mews
Music/video sharing platforms	Advertisement, subscription	Deezer, Netflix, Spotify, YouTube
App stores	Transaction fee	Google Play, Apple app stores
Payment system	Transaction fee	PayPal, ApplePay

Figure 1

(3) A third classification[41] is based on the type of resources to which they grant access: 1) Access to information or content, such as general engines (i.e., Google, TripAdivsor). 2) Access to personal data, such as the social networks (i.e Facebook). 3) Access to goods and/or to services offered by third parties such as online marketplaces (i.e., Amazon, Booking etc, or 'collaborative economy' platforms. (i.e., Airbnb, Uber, Blablacar etc). It is not completely clear whether the new 'collaborative economy' platforms should be treated differently from the already known online market. 3) Access to a workforce or to the expertise capabilities of people (Upwork). 4) Access to money or capital such as crowdfunding sites or payment systems (i.e., paypal). Finally, another categorization is based on network effects of the platforms. [42] In a nutshell, platforms grant access to information, personal data, goods, services, workforce, intellectual capabilities, money, or capital. In the context of digital markets, depending on a platform's business model, users can be buyers of products or services, sellers, advertisers, software developers. The dividing line is, however, not always clear, and that is why the economics of platforms must be studied and understood.

2. The Economics of online platforms.

To understand digital platforms from an economic perspective, one must have some understanding of the concept of value creation on a platform, of the governance system used to orchestrate this value creation, and of the revenue model applied by the platform operator.[43] The value created on a platform comes in the form of communication, information, matching, and choice or diversity.[44] To facilitate value creation and innovation on the platform, the platform operator must install a governance system, reflected in the terms and conditions, comprising behavioural rules and incentives, filters for relevance,

[41] See Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? p.10-11, in Bram Deveolder (ed) 'The Platform economy unravelling the legal status of online intermediaries', (Intersentia 2018)

[42] There are four basic models for operating a digital platform: a) One-sided without network effects, i.e Netflix; b) One-sided with direct network effects, i.e., WhatsApp; c) Two-sided with indirect network effects, i.e., Amazon, Youtube. NY Times; and d) Two-sided with indirect and direct network effects, i.e. Facebook, Linkedin. See Olga Batura et al, "Online platforms and the digital single market. A response to the call for evidence by the House of Lord's internal market sub-committee" in e-Conomics (2015) p. 3

[43] See EU Commission, (2017) *Business-to-Business relations in the online platform environment*, p. 7, available at https://op.europa.eu/en/publication-detail/-/publication/04c75b09-4b2b-11e7-aea8-01aa75ed71a1/language-en accessed 18 May 2020.

[44] Ibid. p. 7

and trust mechanisms (i.e., safe transactions).[45] Here platform act as regulators by setting up the rules through which their users interact[46] and, accordingly, the governance systems serve to avoid negative externalities on participants which reduce the value of the platform to its members.[47] Finally, a platform operator must (eventually) find a revenue model which allows to capture part of the value created on the platform, but which does not conflict with the governance mechanisms.[48]

The platform-based companies Google, Apple, Facebook and Amazon have aggregated power at unprecedented speed and scale: their combined market capitalisation grew from $430 billion in 2010 (roughly the GDP of Poland) to more than $2300 billion in 2017 (roughly the GDP of India, the seventh largest economy in the world). These four 'GAFA platforms' sit at the core of what is becoming a platform society[49], in which a global, corporate infrastructure uses data and algorithms to organise social and economic interactions. In the world of platforms, rather than flowing in a straight line from producers to consumers, value may be created, changed, exchanged, and consumed in a variety of ways and places. The spread of the platform model into one industry after another is causing a series of revolutionary changes in almost every aspect of business. Platforms beat traditional firm because platforms scale more efficiently by eliminating gatekeepers, unlocking new sources of value creation/supply and by using data-based tools to create community feedback loops.[50] Unlike traditional businesses, platforms do not produce anything they do not have to invest directly in the production of the content, goods or service or capital to which they give accesses, instead they rely on the resources

[45] **Behavioural incentives** activate users to contribute to value creation and to act in line with the platforms' strategic objectives. Google, for example, offers free cloud storage in return for reviews of locations on Google Maps. **Filters** are **needed to increase relevance** of e.g. search results, suggestions, or advertisements. Failure to install proper filters may drive users away; e.g. by the end of the 1990s, people massively traded Yahoo for Google as the Google search algorithm was a much better filter. Similarly, **a lack of proper trust mechanisms** may drive users away. Trust should be defined as broadly as possible: trust that information is correct (no fake news, no sponsored search results), **trust that transactions are completed after payment, trust that personal information is not shared with third parties**, etc. Ibid. p. 8.

[46] See Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition Policy for the Digital Era*, available at http://ec.europa.eu/competition/publications, 60.

[47] Amazon's marketplace has a **seller code of conduct** that includes prohibitions against a variety of behaviours such as against trying to damage other sellers or improperly influencing consumer ratings. Google's search engine prohibits websites from many efforts to influence ranking unfairly or essentially gaming its algorithms. See Evans, David S., Vertical Restraints in a Digital World (March 24, 2020). Evans David S., Allan Fels, and Catherine Tucker, eds., *The Evolution of Antitrust in the Digital Era: Essays on Competition Policy* (Boston: Competition Policy International, 2020, Forthcoming). Available at SSRN: https://ssrn.com/abstract=3551597 p. 10-11.

[48] See EU Commission, (2017) Business-to-Business relations in the online platform environment, p. 9, available at https://op.europa.eu/en/publication-detail/-/publication/04c75b09-4b2b-11e7-aea8-01aa75ed71a1/language-en accessed 18 May 2020.

[49] See Jan Konietzko et al, "Online Platforms and the Circular Economy" in N. Bocken et al. (eds.), *Innovation for Sustainability* (Springer 2019) p. 436

[50] For instance, in the traditional publishing industry, editors select a few books and authors from among the thousands offered to them and hope the ones they choose will prove to be popular. It's a time-consuming, labour intensive process based mainly on instinct and guesswork. By contrast, Amazon's Kindle platform allows anyone to publish a book, relying on real-time consumer feedback to determine which books will succeed and which will fail. The platform system can grow to scale more rapidly and efficiently because the traditional gatekeepers—editors—are replaced by market signals provided automatically by the entire community of readers. The elimination of gatekeepers also allows consumers greater freedom to select products that suit their needs. See G. Parker et al, *Platform Revolution: How Networked Markets Are Transforming the Economy---and How to Make Them Work for You*, W.W. Norton & Company 2016, p. 38-44

provided by third parties. In this accessibility-based model, the buzzword is 'access' rather than 'ownership'.[51] Take the music sales industry as an example. The established value configuration (i.e., established innovation) in traditional music sales markets stems from the sale of music files (e.g., Apple iTunes). Conversely, Spotify challenges the aforementioned value configuration. Spotify's value configuration is based on streaming music instead of offering downloads. In this way, Spotify attempts to transform established music value configurations from music ownership to music as a service. From a business model perspective, both music value configurations compete for the same consumers who demand music consumption.[52] This situation is reminiscent of the putting-out system (or "domestic system")[53] and the result is that access replaces ownership. In the words of Sofia Ranchordás, "[Y]ou are now what you can access, and not what you have."[54] However, the rapid growth in the number of online businesses has produced many benefits for consumers and firms as well. It gives consumers reduced search costs,[55] lower prices,[56] reduced information asymmetry (through rating systems, comparison tools) social benefits, easier access to a very wide variety of products and services[57] and attractive delivery conditions.[58] It gives firms[59] the chance of transaction cost reduction, market expansion and access to much more online shelf-space than

[51] See Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? p. 9 in Bram Deveolder (ed) 'The Platform economy unravelling the legal status of online intermediaries', (Intersentia 2018)

[52] See Erol Kazan, *Towards a Disruptive Digital Platform Model*, Copenhagen Business School (2018) p.1

[53] The sharing economy resembles the mercantile model. In this mode of production, which appeared in Europe in the sixteenth century before the manufacturer, farmers would make use of slack periods to perform domestic (often textile) work for merchants with whom they had a commercial relationship. The farmers worked from home, generally using their own tools. In the putting-out system, the merchant also provided the raw materials (the cloth) needed for the activity. This pre-capitalist framework is reflected in many characteristics of current work arrangements via platforms: the disappearance of a workspace managed by the employer, the independence of workers whose relationship with the business intermediary is not hierarchical but commercial, the difficulty of creating a form of collective representation or union, the difficulty of drawing a clear boundary between the domestic and professional spheres, the phenomenon of holding multiple jobs and secondary income activities (which recalls "slashers" – people who combine multiple careers) rather than pursue a single full-time activity, and finally individual self-organization (individuals determine their own level of engagement with the platform). See, *Aurélien Acquier* 'Uberization Meets Organizational Theory. Platform Capitalism and the Rebirth of the Putting-Out System' in Davidson et al, *The Cambridge Handbook of the law of the Sharing Economy*, (Cambridge University Press 2018) p. 19

[54] See Sofia Ranchordás, *Does Sharing Mean Caring? Regulating Innovation in the Sharing Economy*, 16 MINN. J.L. SCI. & TECH. 413, 416 (2015)

[55] Time saving result from research engines alone create a value of **EUR 140 billion** in the EU. See, Bruno Basalisco "Online Intermediaries: Impact on the EU Economy" (Copenhagen Economics 2015) p. 43 available at https://www.copenhageneconomics.com/publications/publication/online-intermediaries-impact-on-the-eu-economy accessed 26 February 2020

[56] Online marketplaces bring benefits to consumer through lower prices **for EUR 1.1 billion** per annum in Europe, or equivalently around EUR 50 per buyer in Europe. Ibid. p 35

[57] Free social networking services, wikis, generalised search services and comparison shopping generate a consumer surplus of EUR 22 billion. Ibid. p. 40

[58] For instance, lower prices due to an increase in supplier competition, which is driven by reduced barriers to entry, especially for small providers, increased transparency and easier supply across geographies. See, Oxera, "Benefits of online platforms. Prepared for Google", October 2015, p. 19-21, available at https://www.oxera.com/wp-content/uploads/2018/07/The-benefits-of-online-platforms-main-findings-October-2015.pdf.pdf accessed 19 February 2020

[59] See Bertin M, "An Economic Policy Perspective on Online Platforms" Institute for Prospective Technological Studies Digital Economy Working Paper 2016/05, pg. 9

any offline shop can offer. [60]

The only estimate of the economic impact of online intermediaries in EU single market was published by Copenhagen Economics (2013) [61] that estimated in total, intermediaries' activities in the EU contributed around € 430 billion to the GDP of the EU 27 in 2012. This is comprised of a direct GDP contribution of € 220 billion and a long-term indirect GDP contribution due to the productivity impact of intermediaries on other firms of €210 billion. This estimate incorporates e-commerce, and in addition the economic value of free services that cannot be captured in traditional GDP estimates, as latter is made at market cost. According to the study, the economic-wide contribution is equivalent to 1.6 % of EU GDP.[62]

The first scholars to deal with platforms, respectively, D. Evans and R. Schmalensse, provide the following economic definition of platforms: 'a digital multi-sided platform has two or more groups of customers who need each other in some way but who cannot capture the value of their mutual attraction on their own and rely on a digital "catalyst" to facilitate value creating interactions between them'. [63] In other terms, a network orchestrator or a catalyst is a company that facilitate a network of users whose activities in turn create value for the company. This business model leverages a phenomenon known as network effects[64], which occur when the value of a good or service increase as the number of people using it increase.[65] Multi-sided platforms are not exclusive to the online world and also exist in the off-line world. A typical example of multi-sided market is newspapers and the media in general. A platform—the newspaper—allows the interaction between readers and

[60] A report estimates that 93% of SMEs using eBay engage in exporting, compared to only 26% of traditional companies which engage in e-commerce without using the services of online marketplaces. In the period 2010-2014 SMEs operating online have increased their cross-border sales in the EU four times faster than those without an online presence. See, Commission staff working document "Online Platforms, (Accompanying the document) Communication on Online Platforms and the Digital Single Market" {COM(2016) 288} p. 12

[61] See Katrine Ellersgaard Nielsen et al "The impact of Online Intermediaries on the EU Economy" Copenhagen Economics (2013) available at https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/6/226/0/The%20impact%20of%20online%20intermediaries%20-%20April%202013.pdf accessed 26 February 2020

[62] See Hosuk Lee-Makiyama and Rositsa Georgieva, "The Economic Impact of Online Intermediaries" in M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers* (Springer 2017) p. 329

[63] David Evans and Richard Schmalenese, "The Antitrust Analysis of Multi-sided Platform Businesses, National Bureau of Economic Research", Working Paper number 18783, (December 2012) p 7: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1482&context=law_and_economics (accessed 17 February 2020) See D. Evans and R. Schmalensse, *Matchmakers. The new economics of multisided platforms*, Harvard Bussiness Review Press, 2016.; David Evans, *Platform Economics: Essays on Multiside Business*, CPI 2011, p. 30-31.

[64] In the light of the increasing importance of digital markets, the concepts of "networks" and "multi-sided markets" were introduced into the German Competition Act emphasising the special role of network effects, see Section 18(3a) of the German Competition Act.; See also Bertin Martens, "An Economic Policy Perspective on Online Platforms", (2016) p. 3

[65] Kellen Zale, 'Scale and the sharing Economy' in Davidson et al, *The Cambridge Handbook of the law of the Sharing Economy*, (Cambridge University Press 2018) p. 40; This can be counter-intuitive, since with traditional business models the opposite can be true, and the value of an exclusive luxury car does not increase – and may actually decrease – if another one is produced (or bought by a neighbour). However, having more collectors (buyers and sellers) on eBay clearly increases the value of the overall platform since the sellers will add inventory and the buyers will provide liquidity to the platform and increase the number of transactions. Unlike traditional businesses, platforms often exhibit network effects, and these have profound competitive implications. See Laure Claire Reillier and Benoit Reillier, *Platform Strategy. How to Unlock the Power of Communities and Networks to Grow Your Business* (Routledge 2017) p. 35

advertisers.[66] Further, when people join networks (be it social networks or telecoms networks), all the other network users benefit since the network's reach – and therefore overall value – is increased. This is a positive externality since all network users are better off as a result. An externality occurs when individuals or firms are impacted, positively or negatively, by an economic transaction that is independent of them.[67] In the context of platform markets, these effects can apply to users who are on the same side (indirect) or on the other side (direct) of the market.

Direct network effects occur when the utility of a user depends on the decisions of other users and all these users belong to a group.[68] Direct network effect can be positive or negative. Typical examples of **positive direct network effects** are communication networks in which everyone can communicate with everyone.[69] Further, participants in a ride-sharing network like Uber benefit because the more people join the network, the more likely drivers will be able to find a passenger in need of rides. Instead, the platform benefit from networks effects as more individuals join a network, the more valuable the platform becomes as far as more commissions from each ride will be collected.[70] Indirectly, the public can benefit if the network may make it more feasible to achieve socially desirable activity that was previously difficult to coordinate (i.e., reduce congestions in case of carpooling apps). Otherwise, negative direct network effects occur when users suffer from increased participation from other users. This may be due to overloading of the platform. For example, traffic congestion for users of an internet service provider.

In contrast to positive direct network effects, the presence of **positive indirect network** effects describes a situation in which one type of economic agent (i.e., users) may value a product more if more of another group of economic agents uses that product as well. This is known as a positive indirect network effect.[71] Positive indirect network effects are often found on e-commerce platforms. To link multiple market players and get the network

[66] The key to the success of a newspaper is indirect network effects. The wider the number of users in each side, the higher the benefit for the other side. On the one side, advertisers will be increasingly interested in the newspaper as it is more widely read. On the other side, readers will be increasingly interested in a newspaper if content is enriched with the revenue generated by a larger pool of advertisers. The platform, the newspaper, has a significant role as it defines the distribution of the benefits derived from the new interaction among all the players: the readers, the advertisers, and the platform itself. If the benefit in terms of higher advertising revenue is not shared with the readers in terms of higher expenditure in quality content (and a lower price for the newspaper), readers will not buy the newspaper. Montero J.J, 2019, Regulating Transport Platforms: The Case of Carpooling in Europe, p. 16, in Finger M. & Audoin M, 2019, *The Governance of Smart Transportation Systems*, Springer International Publishing

[67] See Laure Claire Reillier and Benoit Reillier, *Platform Strategy. How to Unlock the Power of Communities and Networks to Grow Your Business* (Routledge 2017) p. 31

[68] For an introduction to the economics of network effects, see Belleflamme, Paul and Martin Peitz (2018b), *Platforms and Network Effects*, in Luis Corchon and Marco Marini (eds.), *Handbook of Game Theory and Industrial Organization,* vol. II, Edward Elgar, 286– 317.

[69] Here, the benefit of a user depends significantly on the participation decisions of other potential users. Examples include instant messaging apps like WhatsApp or Snapchat, and social networks like Facebook and LinkedIn CERRE Report, (May 2019), *Market definition and Market power in the platform economy*, p 13, available at https://cerre.eu/publications/market-definition-and-market-power-platform-economy/ accessed 6 January 2020

[70] Kellen Zale, 'Scale and the sharing Economy' in Davidson et al, p, 41

[71] It can arise because one type of economic agents (e.g. a buyer, a man, cardholder) wants to search for and transact with another type of economic agent (e.g., a seller, a woman, a merchant) and vice versa. See David Evans, *Platform Economics: Essays on Multiside Business*, CPI 2011, p. 56-57.

effects started, industry platforms all must solve a chicken-or-egg problem (more buyers will attract more sellers to the market, and vice versa). This means that one market side usually needs to come on board first and provide something that attracts another side.[72] In an ordinary linear business model without network effects, the value of a business increases linearly with the number of clients. In a networked business, the value increases exponentially with the number of agents connected to the network. In a networked business, the value increases exponentially with the number of agents connected to the network. The task of the platform organizer is to attract as many users as possible on all sides. [73] If the two groups are mutually connected by cross-group external effects, there are positive indirect network effects on both sides of the market (i.e Tinder, Amazon, eBay).[74] There are also **negative indirect network effects**: one type of economic agent on the network harms another type of agent. For instance, buyers often find advertisements disturbing. From the point of view of an advertiser, more advertising leads to fewer buyers, which is viewed negatively by the advertiser; from the point of view of a buyer, more buyers *ceteris paribus* lead to more advertising, which is judged negatively by the buyer.[75] The platform solves the externality problem between advertisers and consumers by using content to bribe people into viewing ads. Indirect network effects are the key aspect of multi-sided platforms. They are the source of the catalytic reaction—and much of the value—created by the platform. A key practical aspect of these indirect network effects is that they require that the platform "balance" the two sides to maximize the value of the platform to either side. The platform has zero value to either side if the other side is not on board.[76]

Summarising: network effects are very important since they can represent a significant barrier to entry for competitors and therefore contribute to protecting a business. In certain circumstances, network effects may lead a platform to reach a 'critical mass', and even in some markets 'tip' to a 'winner takes all' natural equilibrium, where a single business ends up serving the entire market. [77] Network effects are not just about the number of platform participants, but about their propensity to interact on the platform as well. Inactive users contribute less to network effects on a platform than active ones that participate frequently.[78] On the basis of the benefits highlighted in the literature, the OECD defined the economic role of online platforms as

[72] See Michael A. Cusumano et al, *The Business of Platform. Strategy in the Age of Digital Competition, Innovation and Power*. Harper Business, 2019, p. 52
[73] See Bertin M, "An Economic Policy Perspective on Online Platforms, p. 10
[74] See Demary, Vera and Rusche, Christian, "The economics of platforms" IW-Analysen, No. 12, German Economic Institute Cologne, p. 17.
[75] CERRE Report, (May 2019), *Market definition and Market power in the platform economy*, p 14, available at https://cerre.eu/publications/market-definition-and-market-power-platform-economy/ accessible 6 January 2020
[76] See David Evans, *Platform Economics: Essays on Multiside Business*, p. 57, CPI 2011.
[77] Lundqvist B., Murati E. (2020) Collaborative Platforms and Data Pools for Smart Urban Societies and Mobility as a Service (MaaS) from a Competition Law Perspective. In: Finck M., Lamping M., Moscon V., Richter H. (eds) Smart Urban Mobility. MPI Studies on Intellectual Property and Competition Law, vol 29. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978- 3-662-61920-9_10
[78] See Laure Claire Reillier and Benoit Reillier, *Platform Strategy. How to Unlock the Power of Communities and Networks to Grow Your Business* (Routledge 2017) p. 35

follows:[79] 1) providing infrastructure; 2) collecting, organising, evaluating information; 3) facilitating social communication and information exchange; 4) aggregating supply and demand; 5) facilitating market processes; 6) providing trust.

3. The Rise of the Collaborative Economy.

The collaborative economy, as a sector of the online economy platform ecosystem, is a new triangular business model enabling the exchange of services and the common usage of goods among users registered on an online platform. The combination of technological evolution, urbanization, overpopulation, the financial crisis and the rise of unemployment have resulted in the rapid growth of the collaborative economy.[80] The most widely recognized collaborative economy companies are the "ride share" companies, such as Uber and Lyft, and renting platforms, such as Airbnb. Although sharing economy companies are relatively new, in 2013, the global collaborative economy market was valued at $26 billion, and it is expected to grow to $110 billion soon.[81] While an estimate published in early 2016 posited that the growing sharing economy could reduce under-utilization of assets – i.e., labour, cars, energy finance, and accommodation – by up to €572 billion annually in Europe.[82]

Promoters and makers of sharing economy claim to be transforming society and promoting some form of societal promise in their business model, such as improving access to products and services by disrupting the revenues of big business, building social ties, extending the lifespan of objects, encouraging recycling, etc. In response to these promises, two opposing visions clash among expert and academic observers.[83] On the one hand, "supporters" of the sharing economy describe the sharing economy as an opportunity for individual emancipation and environmental progress, in opposition to the hierarchical power of traditional economic institutions such as large firms – the heirs of the second industrial revolution.[84] On the other hand, opponents criticize the

[79] See OECD (2010), 'The economic and social role of Internet intermediaries', April, p. 15, https://www.oecd.org/internet/ieconomy/44949023.pdf accessed 19 February 2020

[80] Hatzopoulos V, *The collaborative economy and EU law'* (Hart, Oxford 2018) p. 2-3; See Guodin P, "The Cost of Non-Europe in the Sharing Economy" p, 11-13, Study for European Parliamentary Research Service 2016.

[81] See Brett Harris, "Uber, Lyft, and Regulating the Sharing Economy*"*, 41 Seattle U. L. REV. (2017), p. 271

[82] See Pierre Guodin, "The Cost of Non-Europe in the Sharing Economy" Study for European Parliamentary Research Service 2016, p. 6

[83] Author's conclusion is that the sharing economy creates opportunities for innovation that public actors should grasp in order to generate positive outcomes for society. They should politicize the future of the sharing economy, and use it as a tool to promote development, welfare, and well-being rather than an umpteenth version of capitalist power. Further, they suggest that much research needs to be done to understand what type of governance mechanisms and legal statuses may help sustain, over the long term, the hybrid nature of such ventures as they grow. See Acquier A, and Carbon V, 'Sharing Economy and Social Innovation' in Davidson et al, *The Cambridge Handbook of the law of the Sharing Economy*, (Cambridge University Press 2018) p. 51

[84] In reality, what is termed the sharing economy marketplace is controlled by multi-billion dollar corporations with profit-minded goals that have little to do with sharing. See Orly Lobel, 'Coase and the platform economy, in Davidson et al, *The Cambridge Handbook of the law of the Sharing Economy*, (Cambridge University Press 2018) p. 67

sharing economy and the rise of peer-to-peer platforms for being a "low cost" access economy, based on business models that destabilize employment relations, promote a hidden neoliberal agenda, and undermine the very concepts of enterprise and salaried employment. Someone has coined the term "sharewashing," in which platform companies, under the guise of the misleading term "sharing economy," shift liability and risk onto employees and consumers.[85] Additionally, platforms are shaking up some fundamental tenets of the sociological tradition of organizational analysis, as relations of social and economic domination are no longer based on the cleavage between capital and labour.[86] It is true that platform economy encourages a greater level of consumption, it does change consumerism's model by switching the ownership from hotel or cab owners to less institutionalized players. But it does not change the level of ownership required. If the platform economy does not transform consumers' model from owning to borrowing—what is its social innovation?[87]

This phenomenon is known by different labels: the sharing economy, the gig economy, the platform economy, the on-demand economy, the peer-to-peer (P2P) economy and even the Uberized economy. Each of these expressions catches a different, prominent feature of the topic which this book aims to analyse.[88] Each of these terms represents an aspect of the digital platform revolution, but none completely captures the entire scope of the paradigmatic shift in the ways we produce, consume, work, finance, and learn. This new economy dramatically extends the lifecycle of products, shortens time of use, and exponentially expands connectivity and access. Starting with the latter, the Uberized economy refers to the destructuration of the value chain by new intermediaries which, through the use of digital technologies capture part of

[85] See Anthony Kalamar, (13 May 2013) Sharewashing Is the New Greenwashing, https://www.opednews.com/articles/2/Sharewashing-is-the-New-Gr-by-Anthony-Kalamar-130513834.html?p=2&f=Sharewashing-is-the-New-Gr-by-Anthony-Kalamar-130513-834.html Accessed 20 February 2020; So who wins and who loses in the sharing economy? The winners are largely the proprietors of the new technologies and architects of the new service models that characterize the sharing economy.11 However, consumers have often gained as well, to the extent that they are provided with goods and services at lower prices as well as greater choice and convenience. The losers are those whose interests are imbricated in long-established markets which have been destabilized by the advent of the sharing economy: participants in the supply chains that support those markets; consumers who, though benefiting from lower prices, are often unsuspectingly exposed to new risks;14 workers whose employment prospects in traditional enterprises have been radically diminished;15 and a new cohort of operatives enrolled in the legally ambiguous and economically risky work relationships that make possible the consumer choice and lower prices delivered by the sharing economy. Thus, the sharing economy presents problems in many markets, many domains of public policy, and many juridical field. See also Harry Arthurs "The False Promise of the Sharing Economy" in McKee Derek et al Law and the Sharing Economy: Regulating online market platforms, (2018) University of Ottawa Press, Ottawa p. 57

[86] Since 1865 when Marx theorized relations of domination in the capitalist regime, it has been accepted that conflicts concerning value production and value capture revolve around the distinction between capital holders on one side and labour providers (who exchange work for a salary) on the other.[86] Indeed, platform workers, whether Uber drivers or Airbnb hosts, possess (or at least provide) the capital needed to perform their activity. In the strange world of platform capitalism, workers are capitalists without power, exploited by the virtual managers (algorithms) of companies without employees. See, K. Marx, *Salaries, prixet plus value* (2010).

[87] In terms of such innovation, the distributional effect of the P2P is quite difficult to evaluate. On the one hand, by making some services more widely available at reduced prices, the P2P economy arguably promotes increased use of these services by lower-income consumers. See Erez Aloni, "Pluralizing the 'Sharing' Economy" (2016) 91:4 Wash L Rev 1397-1459. (1424)

[88] See Hatzopoulos V, *The collaborative economy and EU law',* p. 4-6. (Hart, Oxford 2018)

the value at the detriment of traditional operators.[89] The P2P economy is as an economic model where people (peers) exchange goods, services, space, and money with each other (C2C) via peer-to-peer platforms.[90] The on-demand economy considers that access to a service or to a good is requested solely when necessary; hence, the remuneration or the price for it is only paid for limited usage, while being neither fixed nor predetermined. To describe the emerging platform economy, some scholars have used the term "platform capitalism", referring "to a set of organizations carrying out productive and for-profit activities through digital platforms that arrange transactions between providers and customers".[91] The platform economy recognizes that the mushrooming of online platforms as virtual marketplaces to match demand and supply amongst peers has been and will be the driving force of the platform economy itself.[92] After all, while the P2P economy emphasizes the role of humans, the platform economy underlines the importance of algorithms and the Internet. The gig economy, in turn, draws attention to an economic system that uses online platforms to digitally connect workers, or "individual service-providers," with consumers.[93] A typical example in this respect is the activity of food delivery.[94] However, the "gig" business model bypasses many of the regular responsibilities and costs of employment, leading to widespread legal ambiguity, which has resulted in challenges as to whether workers should in fact be classified as employee.[95] Finally, the sharing economy, perhaps the most famous expression, indicates a system whereby the involved actors behave differently: an online platform performs the passive role of the matcher of demand and supply while a service provider and a user exploit their respective, often idle, expertise or resources, such as a car ride, baby-sitting, translation, legal advice and household chores. The original idea behind it was not to earn additional income. Until a decade ago, in the golden age of couch-surfing and before the advent of the now-symbolic Uber and Airbnb, online

[89] See Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? p. 4, in Bram Deveolder (ed) 'The Platform economy unravelling the legal status of online intermediaries', (Intersentia 2018)

[90] The P2P economy model includes for-profit and non-profit platforms and peer-to-peer exchanges and business-to-peer exchanges. See, Erez Aloni "Pluralizing the sharing economy." Wash Law Rev 91(4) 2016, p. 1410-1412.

[91] Acquier, A. (2018). Uberization Meets Organizational Theory: Platform Capitalism and the Rebirth of the Putting-Out System. p.14, In N. Davidson, M. Finck, & J. Infranca (Eds.), The Cambridge Handbook of the Law of the Sharing Economy (Cambridge Law Handbooks, pp. 13-26). Cambridge: Cambridge University Press. doi:10.1017/9781108255882.002

[92] See Bram Devolder *The Platform Economy. Unravelling the legal status of online intermediaries,* (Intersentia 2018) Busch C, et al "The rise of the platform economy: a new challenge for EU consumer law?" in EuCML, P. 3-10; See also Isabelle Daugareilh et al, "The platform economy and social law: Key issues in comparative perspective", ETUI aisbl, Brussels 2019, p. 19.

[93] See Harris, B, "Uber, Lyft, and regulating the sharing economy" in Seattle University Law Review, (2017) *41*, 269–285.

[94] See Alex J Wood et al, "Good Gig, Bad Gig: Autonomy and Algorithmic Control in the Global Gig Economy" in Work, Employment and Society 2019, Vol. 33(1) 56–75 . The gig economy consists both of work that is transacted via platforms but delivered locally and thus requires the worker to be physically present, and work that is transacted and delivered remotely via platforms. Local gig work includes food delivery, couriering, transport and manual labour. Remote gig work by contrast consists of the remote provision of a wide variety of digital services, ranging from data entry to software programming (see Table 1), via platforms such as Amazon Mechanical Turk (MTurk), Fiverr, Freelancer.com and Upwork.

[95] James Dugga et al, "Algorithmic management and app-work in the gig economy: A research agenda for employment relations and HRM" in Human Resource Management Journal V. 30. (1) 2020 p. 115

platforms simply helped out to match demand and supply in a passive manner while exchanges were essentially limited. This scenario has now radically changed to the extent that online platforms have moved away from this pioneering attitude and evolved toward a true business model aimed at profit-seeking.[96]

The economic exchange, in its most sophisticated form, can take place, on the one hand, through renumeration, and on the other hand, through so-called freemium mechanisms, whereby users agree to transfer their personal data to an online platform. This economic exchange, be it in a simple or in a sophisticated form, is often transnational and hence covered by the European Union (EU) internal market law. The strength and relevance of intermediary digital platforms has been into the loop of attention by ongoing efforts of the European Union towards a future legal framework for the collaborative economy, namely: the Communication from the Commission on "A Digital Single Market" (DSM Communication),[97] as well as on "A European Agenda for the collaborative economy";[98] the Communication from the Commission on "Online Platforms and the Digital Single Market (Opportunities and Challenges for Europe)";[99] Further, on 15 June 2017, the European Parliament passed a Resolution on a European Agenda for the collaborative economy.[100]

While the EU Parliament [101] used the term 'sharing economy', the Commission itself used the term 'collaborative economy'. The Agenda adopts the following definition for the collaborative economy: "collaborative economy' refers to business models where activities are facilitated by collaborative platforms that create an open marketplace for the temporary usage of goods or services often provided by private individuals'. [102] The collaborative economy involves three categories of actors: (i) service providers who share assets, resources, time and/or skills — these can be private individuals offering services on an occasional basis ('peers') or service providers acting in their professional capacity ("professional services providers"); (ii)

[96] The Internet has decisively contributed to the rapid growth of the collaborative economy, not only by prompting the creation of dedicated website functioning as virtual marketplaces but, more recently, through the availability of apps on everybody's mobile phones. These apps thus work as intermediaries between service providers and users. See Inglese M, *Regulating the Collaborative Economy in the European Union Digital Single Market* (Springer 2019) P 8-9.

[97] A DSM is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. See, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, "A Digital Single Market Strategy for Europe", COM(2015) 192 final.;

[98] European Commission, 'A European agenda for the collaborative economy', COM (2016) 356 final.

[99] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions "Online Platforms and the Digital Single Market Opportunities and Challenges for Europe" COM(2016) 288 final.

[100] Press Releases, Sharing economy: Parliament calls for clear EU guidelines, https://www.europarl.europa.eu/news/en/press-room/20170609IPR77014/sharing-economy-parliament-calls-for-clear-eu-guidelines

[101] Defined as "The use of digital platforms or portals to reduce the scale for viable hiring transactions or viable participation in consumer hiring markets (i.e. 'sharing' in the sense of hiring an asset) and thereby reduce the extent to which assets are under-utilised." See, Pierre Guodin, "The Cost of Non-Europe in the Sharing Economy" Study for European Parliamentary Research Service 2016, p. 5

[102] See European Commission, 'A European agenda for the collaborative economy', COM (2016) 356 final. p. 3-4

users of these; and (iii) intermediaries that connect — via an online platform — providers with users and that facilitate transactions between them. Collaborative economy transactions generally do not involve a change of ownership and can be carried out for profit or not-for-profit.

In its public consultation on online platforms the Commission's report highlighted the concerns and issues that impact collaborative economy development. Uncertainty over the rights and obligations of users was the most cited potential obstacle to the growth of the collaborative economy across all respondent groups. Additionally, all respondent groups voiced concerns about the insufficiently adapted regulatory framework. Fragmented markets, created by overly strict or unsuitable regulation favouring incumbents, were by far the most frequently mentioned barriers to the development of the collaborative economy. Uncertainty about the employment status, i.e., whether providers are self- employed or employees, was also mentioned. Moreover, a regulatory environment adapted to the collaborative economy and support for innovation and entrepreneurship were cited as desired actions. Most respondents considered European action promoting the collaborative economy necessary.[103] Indeed, the emergence of the sharing economy has taken European regulators by surprise. At present, uncertainty reigns not only with respect to *how* this phenomenon should be addressed but also *by whom* – whether the EU should issue regulations or leave this to the Member States.[104]

Following the Commission's above definition of the collaborative economy, to Hatzopoulos the term collaborative economy encompass those *stricto sensu* collaborative economy platforms, which facilitated: a) access, as opposed to transfer of ownership; and b) the conclusion of transaction (contract) between two other parties (a triangular relationship); c) which parties are mostly- but not exclusively - peers, regardless of whether these are prosumers or service providers.[105] Therefore, according to him the term 'collaborative economy' is preferred over the others mentioned above for three main reasons. First, the collaborative economy' is broader than the term 'sharing economy'. The collaborative economy refers to an economic model that focus on providing access to products and services through renting, trading or sharing instead of traditional ownership. The sharing economy is a subset of the collaborative economy that focuses solely on the outright sharing of assets. Thus, the more restricted term 'sharing economy' would exclude platforms, like Uber, which facilitate transportation services other than ridesharing per se. Second, the term collaborative economy is more ideologically neutral. Third, it is the official name adopted by the European Commission.[106]

Likewise, according to Inglese, the expression 'collaborative economy' is

[103] See, Synopsis Report on the public consultation on the regulatory environment for platforms, online intermediaries and the collaborative economy, available at https://ec.europa.eu/digital-single-market/en/news/full-report-results-public-consultation-regulatory-environment-platforms-online-intermediaries accessed 13 February 2020

[104] There are no legal obstacles for the EU to regulate sharing economy platforms yet given the specific characteristics of the sharing economy, regulation at smaller scales will often be preferable. See. M Flick, "The Sharing Economy and the EU", in Davidson et al, *The Cambridge Handbook of the law of the Sharing Economy*, (Cambridge University Press 2018) p 261.

[105] Hatzopoulos V, *The collaborative economy and EU law'* (Hart, Oxford 2018) p. 7

[106] Ibid, p. 4-5

preferred [107] over the others mentioned above because it implies that exchanges effectuated among peers and intermediated by online platforms can be carried out for free or against remuneration.[108] However, it is only when the latter condition is satisfied that EU fundamental economic freedoms come into play. Otherwise, the "Cambridge Handbook on the law of the sharing economy" [109] uses the term "sharing economy" because it is the most ubiquitous term for referring to a myriad of new mechanisms for facilitating the exchange of goods and services, often provided by individual, small-scale actors. The Handbook embraces a very broad conception of the "sharing economy," including large for-profit firms like Airbnb, Uber, Lyft, Taskrabbit, and Upwork, as well as smaller, non-profit collaborative initiatives, including lending libraries, maker spaces, and fab labs, through which individuals can obtain temporary access to a particular resource. In this view, this research refers to the notions such as "the sharing economy," "the platform economy," and the "collaborative economy" as interchangeably.

3.1 Main characteristics of the Collaborative Economy.

3.1.1 Triadic Relationship and Platform Trust.

Some online and collaborative platforms, pursue their own commercial interests and, because of their multi-sidedness, they have to cater to both businesses as well as consumers.[110] In the legal field, triangular commercial relations are not uncommon, nor is their widespread presence imputable solely to the advent of the Internet. Indeed, it suffices to recall the well-established figure of commercial agents, executing a business on behalf of a principal and concluding it with a third party. [111] However, what distinguishes the collaborative economy from any other sort of triangular legal relation is the

[107] Lacking remuneration, EU internal market law cannot be triggered. See Inglese M, *Regulating the Collaborative Economy in the European Union Digital Single Market*; p.11, (Springer 2019)

[108] See, Juliette Sénéchal: "The Diversity of the Services provided by Online Platforms and the Specificity of the Counter performance of these Services — A double Challenge for European and National Contract Law", in EuCML (2016) p. 41.

[109] The phrase "sharing economy" has faced significant criticism. As numerous commentators have observed, highly visible and often controversial firms like Uber, Lyft, and Airbnb, which are often referred to as part of the sharing economy, do not, in fact, facilitate the gratuitous sharing of goods and services. Rather they facilitate commercial transactions between two parties: sellers or providers of goods and services and buyers or users. For this reason many prefer the term peer-to-peer, which suggests that, in most cases, the parties on either side of these exchanges are not professionals and that, in many cases, their activity is simply a side gig that makes use of the spare capacity of a resource they already own. But this description proves inaccurate for a significant number of providers, as some individuals work full time as a driver for Uber or Lyft or rent out multiple apartments on Airbnb. Others prefer the term platform economy, which focuses on the digital platforms and apps through which transactions are brokered. In many instances these platforms enable users to obtain goods and services "on demand." But this term can also be under-inclusive, as it may fail to include those components of the broader sharing economy that do in fact reflect a traditional understanding of "sharing," such as neighbourhood tool libraries, which also may not rely upon a digital plat- form to facilitate exchanges. Cognizant of these limitations the Handbook had preferred the above term. See Nestor M. Davidson et al *The Cambridge Handbook of the law of the Sharing Economy*, (Cambridge University Press 2018) p. 2-3

[110] See Graef, I., Jeon, D-S., Rieder, B., van Hoboken, J., & Husovec, M. (2021). *Work stream on differentiated treatment,* Final report. European Commission., p. 11 https://platformobservatory.eu/app/uploads/2020/07/03DifferentiatedTreatment.pdf

[111] See Inglese M, *Regulating the Collaborative Economy in the European Union Digital Single Market* p. 12, (Springer 2019)

diriment role of online platform provider. Considering the asymmetric positions of those three parties, a collaborative economy triangle can be construed as follows. Online platform providers are situated at the apex, on the intuitive ground that, lacking their intermediary role, the collaborative economy cannot exist.[112] Platforms of the collaborative economy belong in the extended family of online platforms.[113] However, what qualifies as an online platform, as it was discussed above, is hotly debated issue (Section 2 above). Otherwise, material providers (i.e., transport or accommodation providers, etc) and users represent the basis of, and maintain, a binary mutual relation between them, while, at the same time, addressing themselves to an online platform provider for different reasons (i.e., to seek redress in the case of wrongdoing perpetrated by providers). For a depth analyses of the other two parties, (i.e., service providers and users) within the EU law context this book is suggested for consultation.[114] Regarding the user, it is worth underlining that the emergence of the collaborative economy has given birth of what is called a 'novel economic agent', characterized by 'decentralisation and de-professionalisation', hence giving rise to the concept of peer and/or prosumer, as a person combining production and consumption.[115] In a nutshell, the key feature is that platforms allow the supply side (the suppliers) to meet the demand side (the customers), creating a triangular structure that is based on relations between (1) the platform and the supplier, (2) the platform and the consumer, and (3) the supplier and the customer. From a legal point of view, this triangular structure is the fundamental aspect of (some) digital and collaborative platforms.

Subsequently, as in any (online or offline) business setting, the presence of trust is a major precondition for successful transactions in the sharing economy. In placing people and human interactions at its core, the sharing economy (or better the platform provider seeks to mitigate our inherent stranger-danger bias by designing and facilitating trust-building capacities between strangers whose interactions are enabled through digital platforms.[116] Trust has traditionally been portrayed as a dyadic relationship between a trustor and a trustee; yet, in many transactions associated with the sharing economy, at least three parties are involved: the (digital) platform provider, and a pair of peers acting on that platform. Based on the triadic

[112] See Sorensen MJ (2016) Private law perspectives on platform services. Eur Common Mark Law 5(1):15–19

[113] See Hatzopoulos V, *The collaborative economy and EU law'* (Hart, Oxford 2018) p. 9

[114] See Inglese M, *Regulating the Collaborative Economy in the European Union Digital Single Market*, p.15-19, (Springer 2019)

[115] See Smorto G (2017) 'Critical assessment of European agenda for the collaborative economy. In depth analysis for the IMCO Committee' IP/A/IMCO/2016-10, PE 595.361, P. 12; *Il consumatore, attualmente, è un soggetto «iper-connesso», che (ri)organizza la propria vita attorno alle applicazioni e agli apparecchi resi disponibili dagli operatori del mercato digitale. La «iper-connessione» consiste nell'uso della tecnologia come «protesi» dell'azione umana per raggiungere decisioni efficienti. Per cui, il consumatore oltre che* ***iper-connesso*** *è anche* ***iper-efficiente****, nei suoi consumi energetici come in quelli digitali, nel senso che adotta decisioni efficienti anche se queste non sarebbero «naturalmente» le sue.* See. Fabiana Di Porto "Dalla convergenza digitale-energia l'evoluzione della specie: il consumatore iper-connesso" in Mercato Concorrenza Regole (Fascicolo 1, Aprile 2016) p. 59-60

[116] See Mareike Möhlmann and Andrea Geissinger "Trust in the Sharing Economy Platform-Mediated Peer Trust" in Davidson et al, *The Cambridge Handbook of the law of the Sharing Economy*, (Cambridge University Press 2018) p. 28

nature of platform-mediated peer trust, a distinction could be made between interpersonal and institutional trust.[117] Sharing economy platforms constantly introduce new and innovative trust cues that support the trust-building process.[118] Consequently, it can be argued that such trust cues are cumulative in nature: The more cues a sharing platform provides, the more likely it is that trust is produced. These cues are leveraged to establish trust in digital platforms in general, and in the sharing economy in particular:[119] a) peer reputation, b) digitalized social capital; c) Provision of information, d) Escrow services; e) Certification and external validation; f) Insurance cove.

3.1.2 Collaborative Platform's Business Models.

Platform businesses may be defined as "businesses creating significant value through the acquisition and/or matching, interaction and connection of two or more customer groups to enable them to transact".[120] Within the sharing economy, by mapping the value creation mechanisms and value distribution mechanisms four types of business model had been identified.[121] The first business model is made by "Commoners" which create and provide free access to public goods by pooling resources and skills in order to make them available to as many people as possible and to spur the emergence of alternative and non-market values, such as open knowledge, free and open access, or do-it-yourself (DIY). Value is created by and for the community or the initiative's ecosystem. Typical example is Wikipedia. The second category is made of "Mission-driven platforms", which intermediate between peers through a digital platform to support a societal cause. Like Commoners, they pursue a mission to transform society through the initiative by facilitating new practices of consumption, exchange, and relationships. The cause and values that initially motivated the founders constitute the purpose of the initiative, which grows along with the volume of resources that are shared through the platform.

[117] **Interpersonal trust** lies at the core of trust in the sharing economy since it refers to relationships between peers acting on these platforms. The sharing platform provider is an enabler for interpersonal trust, while at the same time being dependent on being perceived as a trustworthy institution itself. As the sharing economy is based on human interactions, the interpersonal trust element is arguably more significant than in other online transactions, such as e-commerce. Sharing economy activities tend to be characterized by greater social interaction among peers, as when driving in a car together or spending the night in a host's apartment and having dinner together, than in the more impersonal transactions conducted on platforms such as eBay and Amazon. On the other hand, sharing economy platforms must also establish **institutional trust** as platforms engage in more traditional organization–customer relationships with participating peers. Ibid.

[118] Trust in a platform provider or brand as an organization leads to trust in the peers with whom one is sharing, allowing spillover effects between different trust entities. In particular, such trust hierarchies may be evident at early stages of trust relationships, when users have little familiarity with a sharing economy service. We expect the process of trust transfer to apply as well to low levels of trust. Thus, trust can also be lost by the same mechanism. For instance, public scandals, such as those that have recently affected Uber, might affect the brand of a sharing economy platform, and, in turn, lower consumers' trust in the platform more generally. Ibid. p. 32-33

[119] For instance, peer ratings offer opportunities to access digital social capital accumulated by other members of an online sharing platform. More recently, sharing economy platforms have implemented two-way ratings, or so-called simultaneous reviews, to deal with reciprocal peer review behaviour, which has been shown to result in inflated and non-credible review scores. Ibid, p. 34

[120] See Laure Claire Reillier and Benoit Reillier, *Platform Strategy. How to Unlock the Power of Communities and Networks to Grow Your Business* (Routledge 2017) p. 22

[121] See Acquier, A., & Carbone, V. (2018). Sharing Economy and Social Innovation. p. 54-58, In N. Davidson, M. Finck, & J. Infranca (Eds.), The Cambridge Handbook of the Law of the Sharing Economy (Cambridge Law Handbooks, pp. 51-64). Cambridge: Cambridge University Press. doi:10.1017/9781108255882.005

Typical example is Couchsurfing. In the third category belongs, "shared infrastructure providers" which are for-profit initiatives that monetize access to a strategic proprietary resource. Operating on a membership fee or pay-per-use basis, shared infrastructure providers earn a profit and gain power from a proprietary infrastructure that individuals and professionals use to realize their projects. Typical example is ZipCar. The last business model and the most visible and controversial initiatives in the sharing economy are known as "Matchmakers". These are for-profit commercial platforms that bring individuals together in networks so they can exchange goods or services on a peer-to-peer basis. In the field of personal transport or accommodation, examples include platforms such as Uber, Airbnb, and BlaBlaCar. The platform intermediates between peers and captures part of the value created to make a profit from this intermediation. In other terms, economic analyse could characterize the specificities of online platforms. For an in depth analyse of economics of collaborative economy these two books[122] are recommended.

3.1.3 Matching and Management via Algorithms.

A key characteristic of online platforms is their capability to match a very large number of users in a market to facilitate an exchange. Platforms help users of different sides of the market (sellers, buyers, social media users, advertisers, software developers, etc.) to find what they are looking for. The more efficient the platform is in matching users; the more users will be attracted to the platform.[123] Matching in the digital context is facilitated by matching or search algorithms. This efficiency is gained thanks to aggregation and analyse of data, it follows that the input of large amount of data in platforms (algorithms) reduces the search cost for users and, therefore, improving better matching.[124] Usually, algorithms are presented as objective, neutral, even benevolent. However, numerous applications have shown that algorithms are not pure mathematics, infallible and neutral, but rather human opinions structured in mathematical form and often reflect the pre-understandings of those who design them, or the historical series taken as a reference. The fact is that blind faith in the algorithm is leading to a rather disturbing expansion of its domain, accompanied also by the first doubts about its actual impartiality. Uber and other ride-hailing apps uses algorithms and applied it to work, and that is not always a good thing. For Uber drivers, the workplace can feel like a world of constant surveillance, automated manipulation, and threats of "deactivation." [125] In specific, the use of technology and algorithms as substitutes to direct managerial control creates power asymmetries between the platform and the worker (i.e., Uber's driver) in the collaborative economy. Such algorithms may be used, as in the case with *Uber,* to assign work, in order to fix prices, in order to evaluate and control the worker performance on the basis of users' rating, acceptance/cancellation rate.

---

[122] Ming Hu, *Sharing Economy Making Supply Meet Demand* (Springer 2019); See also, Elena G. Popkova, Bruno S. Sergi, *Digital Economy: Complexity and Variety vs. Rationality* (Springer 2020).

[123] See Bertin M, "An Economic Policy Perspective on Online Platforms" Institute for Prospective Technological Studies Digital Economy Working Paper 2016/05, p. 20.

[124] See Hatzopoulos V, *The collaborative economy and EU law* P.12

[125] Alex Rosenblat (12 October 2018) *When Your Boss Is an Algorithm*, available https://www.nytimes.com/2018/10/12/opinion/sunday/uber-driver-life.html accessed 13 February 2020

The algorithms may be further used to perform a series of managerial and/o supervisory tasks as speeding up the work process, determining the timing and length of breaks, monitoring quality, ranking employees and more. The automatic "termination" of workers when their ratings fall below a certain level (4.6 out of 5 stars in the case of *Uber)* or "firing by algorithms" is the most extreme of manifestation of algocracy. [126] Management-by-algorithm, or algorithmic management, is commonplace within collaborative economy. Algorithmic management can be defined[127] as "a system of control where self-learning algorithms are given the responsibility for making and executing decisions affecting – *not exclusively* (emphasises added) - labour, thereby limiting human involvement and oversight of the labour process". It replaces some of the tasks and processes that workers typically engage with by using algorithms that are developed by the very same individuals' data on the platform.

The autonomy resulting from algorithmic control can lead to overwork, sleep deprivation and exhaustion because of the weak structural power of workers vis-a-vis clients. This weak structural power is an outcome of platform-based rating and ranking systems enabling a form of control which can overcome the spatial and temporal barriers that non-proximity places on the effectiveness of direct labour process surveillance and supervision. [128] In a nutshell, most platforms heavily rely on automated algorithm-based decision-making to process transactions and data. Automated decision-making systems are efficient and often more impartial than human decision makers. But they can also perpetuate discrimination and deleteriously affect citizens. From a legal perspective protection, Art. 22 GDPR on automated individual decision-making, including profiling, plays a crucial role here to avoid undesired effects on citizen and businesses. [129]

4. Legal challenges arising from the platform economy in the internal market.

According to a public consultation [130] carried out by the European Commission, the most commonly undesired practices experienced by businesses in their relationship with platforms were: (i) a platform applying unbalanced terms and conditions; (ii) a platform promoting its own services to the disadvantage of services provided by suppliers (self-preferencing); and (iii)

---

[126] See Hatzopoulos V, *The collaborative economy and EU law*, p-154-155; Algocracy means governance by computer algorithms, instead of bureaucratic rules of surveillance. It was used for the first time by Anesh A, *Virtual Migration. The Programming of Globalization*, (Duke University press 2006) p 5.

[127] See James Dugga et al, "Algorithmic management and app-work in the gig economy: A research agenda for employment relations and HRM" in Human Resource Management Journal V. 30. (1) 2020 p. 119.

[128] See Alex J Wood et al, "Good Gig, Bad Gig: Autonomy and Algorithmic Control in the Global Gig Economy" in Work, Employment and Society 2019, Vol. 33(1) p. 70

[129] See Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 available at file:///C:/Users/erion/Downloads/wp251rev01_enpdf.pdf accessed 6 January 2020

[130] European Commission (2016). Public consultation on the regulatory environment for platforms, online intermediaries and the collaborative economy. Synopsis Report. P. 9 Available at https://ec.europa.eu/digital-single-market/en/news/results-public-consultation-regulatory-environment-platforms-online-intermediaries-data-and accessed 27 February 2020

a platform refusing access to its services. When policymakers face innovation in the way people transact, exchange goods, and deliver services, they must decide whether and which legal rules apply. Some existing regulations lend themselves quite easily to direct application on the platform. Other regulations appear outdated.[131] Online platforms can create and shape new markets, to challenge traditional ones, and to organise new forms of participation or conducting business based on collecting, processing, and editing large amounts of data.[132] Thus, digital platforms obviously challenge the law, and this is a key feature and consequence of their operation.[133] Most platforms are challenging specific laws (market access,[134] data protection,[135] competition law,[136]

[131] When regulation is designed to address distributional concerns, such as equality and fairness goals, it is likely that some of the issues that pervaded offline exchanges will continue into platform relationships. The platform economy thereby offers a fresh opportunity to observe and analyze the fit between goals and actual outcomes of a range of existing laws. When laws do not promote social goals but instead protect incumbent industries against competition, the platform is clearly a welcome intervention and such anticompetitive laws should largely be deemed obsolete. Innovation should also be viewed as an opportunity to unpack, and rethink, traditional regulatory categories. See Lobel, O. (2018). Coase and the Platform Economy. p. 71, In N. Davidson, M. Finck, & J. Infranca (Eds.), The Cambridge Handbook of the Law of the Sharing Economy (Cambridge Law Handbooks, pp. 67-77). Cambridge: Cambridge University Press. doi:10.1017/9781108255882.006

[132] Communication from the commission to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions on "Online Platforms and the Digital Single Market Opportunities and Challenges for Europe", SWD(2016) 172 final P. 2

[133] See Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? p.2 in Bram Deveolder (ed) 'The Platform economy unravelling the legal status of online intermediaries', (Intersentia 2018)

[134] A key question for authorities and market operators alike is whether and if so to what extent, under existing EU law, collaborative platforms and service providers can be subject to market access requirements. These can include business authorisations, licensing obligations, or minimum quality standard requirements (e.g. the size of rooms or the type of cars, insurance or deposit obligations etc.). Under EU law, such requirements need to be justified and proportionate, taking account of the specificities of the business model and innovative services concerned, while not favouring one business model over the other. See, Communication from the commission to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions on "A European agenda for the collaborative economy" (SWD (2016) 184 final). P.3

[135] *Le piattaforme dell'economia collaborativa basano il proprio successo imprenditoriale sulla raccolta di dati dei propri utenti, al fine di individuare le loro preferenze e offrire così un servizio personalizzato. Le pratiche commerciali delle piattaforme dell'economia collaborativa saranno profondamente influenzate sotto diversi aspetti dal GDPR. Novità quali il diritto alla portabilità dei dati potrebbero condurre le piattaforme a collaborare tra di loro, al fine di creare sistemi informatici all'insegna dell'interoperabilità, a vantaggio dell'utente che potrà quindi passare da un operatore all'altro senza ostacolo alcuno. La necessità del consenso preventivo dell'interessato al trattamento dei propri dati personali dovrebbe andare parimenti a beneficio dei consumatori. Permangono tuttavia numerose perplessità; non è infatti chiaro come sarà effettiva- mente garantita la portabilità dei dati, ove i gestori delle piattaforme rifiutassero di collaborare tra di loro, rivelando i propri sistemi e progetti.* See, Mirko Forti, "Le piattaforme online alla prova del Regolamento (UE) 2016/679. Quali tutele per la condivisione dei dati nell'economia collaborativa?" in Rivista di Diritto dei Media (2/2019) P. 15

[136] Platforms generate regulatory concerns because of their expanding market power. Many platform markets tend towards domination by one or very few players, thanks to, among other things, strong network effects and economies of scale advantages, and the exclusive access to vast amounts of consumer, business and transactional data. These data troves give them a constantly self-reinforcing knowledge edge with regards to market dynamics over competitors and regulators alike. See, See Paul-jasper D, "Online platforms and how to regulate them: an EU overview" policy paper no. 227 14 June 2018, in Jacques Dolers Institute Berlin. p. 4.

copyright, taw law,[137] antidiscrimination law,[138] licensing regimes,[139] etc.) and authorities[140] (competition authorities, data protection authorities, judiciary, etc.). In European Union legal context, the CJEU involvement, on the one hand, in the data protection field with rulings on the 'right to be forgotten'[141] and the Schreem I[142] and Schreem II[143] and, on the other hand, concerning the liability legal regime of Uber, Airbnb and Star Taxi App, suggest that there is concrete conflict going on between platforms and the current EU regulatory framework. Another example of this clash is the legal status classification issue faced by sharing economy workers globally. Facing traditional regulation, sharing economy companies and gig workers platforms often default to the argument

[137] The long-standing taxation principle of permanent establishment and physical presence creates loopholes when applied to digital business activities. A government's current taxing rights on corporate income are based on the physical presence of a firm in its jurisdiction. Companies that have only a significant digital presence in a country are free from taxation liability because of lack of legal nexus under the international rules. Facebook has over 2.3 billion monthly users spread over nearly every country, but it pays little or no tax in many countries where it does not have an office. Responding to the pressing call to update tax systems to address business activities in the digital economy, countries have begun to take measures unilaterally. Some countries have broadened the concept of permanent establishment and physical presence to justify taxation of corporate income following the significant economic presence proposal. *Saudi Arabia has established* ***virtual service permanent*** establishment rules. Israel has imposed a corporate tax on non-resident companies with a "significant digital presence." The United Kingdom announced a digital service tax in Finance Bill 2019/20, which becomes effective on April 20, 2020. The taxable income is the value of the advertising sales targeted at U.K. users and the commissions for a transaction with U.K. users. The European Commission has also proposed a 3 percent tax on digital businesses' portion of annual worldwide revenues attributable to European Union (EU) users. The EU's digital service tax proposes allocating revenue in proportion to how often an advertisement has appeared on users' devices and the number of users who conducted transactions on a digital business platform. See, Rong Chen "Policy and Regulatory Issues with Digital Businesses" in World Bank Group (Policy Research Working Paper n. 8948, July 2019) p. 9-12.

[138] Bilateral relationships directly concluded by the parties fall within the scope of those (antidiscrimination) Directives, excluding the triangular one that arises when a digital platform intervenes. They contemplate 'one sided' rather than 'two sided' markets. In particular, platforms face two legal situations: first of all, they may act solely as intermediaries and, secondly, they may add to their brokerage role a range of service components inherently linked to exercising decisive influence over them. If such services imply 'control' of providers, then the online platform in fact becomes "the provider" of the service at hand. In this case, there is no longer a 'two sided market' relationship. Consequently, European non--discrimination rules need to be applied as if there were just two contractual parties without the brokerage of the online platform. However, if the platform acts purely as the go between, for instance cases where Airbnb or Uber are involved, the matter unfolds differently. Indeed, the platform does not discriminate users; rather, suppliers discriminate customers or, vice versa, users discriminate themselves. See, Susana Navas Navarro 'Discrimination and Online Platforms in the Collaborative Economy' in EuCML 2019, p. 36

[139] See Derek McKee "Peer Platform Markets and Licensing Regimes" in McKee Derek et al *Law and the Sharing Economy: Regulating online market platforms*, (2018) University of Ottawa Press, Ottawa p.17

[140] See Altain Strowel and Wouter Vergote, 'Digital platforms: to regulate or not to regulate? p.2 in Bram Deveolder (ed) 'The Platform economy unravelling the legal status of online intermediaries', (Intersentia 2018)

[141] CJEU, 13 May 2014, C-131/12 (Google Spain v AEPD and Marioa Costeja Gonzales).

[142] CJEU, 6 October 2015, C-362/14 (Maximilian Schrems v Data protection Commissioner); Under the safe harbour regime, established by the ECD, 'information society service providers' performing mere conduit, caching and hosting are exempted from liability for third parties' unlawful conduct as long as they are in no way involved with the information transmitted, or, in the case of hosting services, do not have knowledge or awareness of the illegal activities and, if acquired, promptly act to stop them. The regime of 'conditional' liability was envisaged as one of the means necessary for the development of online services and the flourishing of the information society (p. 295). See, Montagnani, Maria Lillà and Trapova, Alina, "Safe Harbours in Deep Waters: A New Emerging Liability Regime for Internet Intermediaries in the Digital Single Market" (July 28, 2018). International Journal of Law and Information Technology, Volume 26, Issue 4, 1 December 2018, Pages 294–310. Available at SSRN: https://ssrn.com/abstract=3221520 or http://dx.doi.org/10.2139/ssrn.3221520

[143] CJEU, 16 July 2020, C-311/18, Data Protection Commissioner v Facebook Ireland

that they are not employers because they are merely offering an online platform that connects workers—or independent entrepreneurs—to consumers.[144] For instance, in United Kingdom, the UK Employment Tribunal[145] (also upheld by the Employment Appeal Tribunal[146]) and France's Court of Cassation [147] reached the conclusion that Uber drivers qualify as workers. Subsequently, the discussion surrounding the collaborative economy triangle is permeated by the ambiguities regarding the nature of the transactions and the identities of the actors.[148] These uncertainties are counterweighted by two certainties. First, online platforms are in a predominant position, being placed at the apex of the collaborative economy triangle and, consequently, exercising decisive control over transactions, payment systems, rate-and-review mechanisms, etc.[149] Second, online platforms have become a matrix not only allowing the conclusion of the main service contract, but also performing part of the main service or, alternatively or cumulatively, performing services related to the main service that the provider does not know how to, is unable to or is unwilling to carry out.[150]

4.1 Defining the Legal status of collaborative platforms in the internal market: intermediaries or real service providers?

Traditional EU regulation, which focus mainly on balancing the interest of two contracting parties, is now confronted with a triangular relationship between a platform, a supplier and a user. Legislators, judges and lawyers across the globe are struggling to determine the legal status of online intermediaries.[151] In general, online platforms are not designed to provide their own accommodation or transport services, but to facilitate the contracting of services provided by third parties. However, the intermediation service provided by platforms is particularly powerful. Indeed, even the notion of internet intermediaries, defined by the OECD[152] as entities that 'bring together or facilitate transactions between third parties on the Internet', is increasingly replaced in common parlance by the more palatable term of "platform", which evokes a role that goes beyond one of mere messenger or connector, and

[144] Critics of this argument point out that the sharing economy companies still manage their workers as if they were employees in various ways, such as unilaterally setting rates for services; dictating how the services are provided; and screening, testing, training, evaluating, promoting, and disciplining the workers based on standards set by the companies. See Brett Harris, "Uber, Lyft, and Regulating the Sharing Economy", 41 Seattle U. L. REV. (2017), p. 274.

[145] *Aslam et al., v. Uber BV et al,* No. ET/2202550/15, https://www.judiciary.uk/wp-content/uploads/2016/10/aslam-and-farrar-v-uber-reasons-20161028.pdf

[146] The Tribunal's finding about drivers not being able to grow their own business or negotiate terms with passengers, impact he capacity for drivers to act on their own entrepreneurial spirt. See, Aslam et al., v. Uber BV et al., NO. UKEAT/0056/17DA, https://www.employmentcasesupdate.co.uk/site.aspx?i=ed36468;

[147] Judgment n ° 374 of March 4, 2020, UberBV V. A..X. https://www.courdecassation.fr/IMG/20200304_arret_uber_english.pdf

[148] See M Inglese, *Regulating the Collaborative Economy in the European Union Digital Single Market* (Springer 2019) p. 20.

[149] This control may be quite limited and concerns data that users submit when creating an account or using a platform such as Facebook or Twitter.

[150] See J Sénéchal "Online Platforms under French Law" cit. p. 128-133

[151] See preface, B. Deveolder (ed.), The Platform economy unravelling the legal status of online intermediaries, New York, 2018.

[152] See OECD, The economic and social role of Internet intermediaries, at oecd.org, 9.

extends to the provision of a shared space defined by the applications within which users can carry out their activities and generate value. If online platforms were required to be pure intermediaries, Airbnb, BlaBlaCar, Amazon, Netflix or Facebook would not be considered online platforms.[153]

In the specific context of the collaborative economy, platforms have become a matrix not only allowing the conclusion of the main service contract, but also performing part of the main service or, alternatively or cumulatively, performing services related to the main service that the provider does not know how to, is unable to or is unwilling to carry out.[154] For instance, companies such as Uber, Lyft, Airbnb, Aereo [155] have been running against existing regulations and the legal battles often turn on how to define the platform business. [156] Acting as an intermediary has several advantages [157] for the platform and it is usually expressed in the platform operator's terms of service. Nevertheless, it is doubtful whether such a declaration is sufficient for reducing the role of the platform to an intermediary. The EU Commission had underlined that whether an online platform also provides the underlying service has to be established on a case-by-case basis. [158] In short, one of the first regulatory challenge around online platforms is to define their legal status: mere facilitator, broker or supplier of integrated service? To put it in EU internal

[153] See Oxera, "Benefits of online platforms. Prepared for Google", October 2015, p. 14-5, https://www.oxera.com/wp-content/uploads/2018/07/The-benefits-of-online-platforms-main-findings-October-2015.pdf.pdf accessed 24 February 2020

[154] See Juliette Sénéchal "Online Platforms under French Law" in U Blaurock (eds) *Plattformen* (Nomos 2018) p. 128-133

[155] In a different field of consumption, media content, the Supreme Court ruled in 2014 that Aereo, a provider of online streaming technology, was an illegal service operating in violation of copyright law. Aereo sought to allow individuals to shift from ownership to access. It developed a bank of tiny antennas in each city in which it operated, which received local TV broadcast signals, much like old rabbit ears. Every time a subscriber wanted to watch or record a show, Aereo assigned an individual antenna to the subscriber. Aereo, viewed through the lens of the platform, was basically a **cloud-based intermediary**, enabling people to intercept what they were free to consume directly. Instead of consumers purchasing an enormous cable package and not watching seventy percent of the channels, and some of the preferred content is unavailable in their cable zone, Aereo provided a cheaper and more fine-tuned option. Moreover, Aereo helped to reduce the barriers to entry for small, in- dependent broadcasters, who aired niche television content that broadcasters and cable companies ignored. The challenge was that, in reality, users who subscribed to Aereo could intercept the local television package of any city in which Aereo operated, regardless of the user's location. Unsurprisingly then, much like other incumbents challenged by the platform, the broadcasting networks opposed this new business model and claimed that it violated their rights to receive transmission fees under the Copyright Act. In 2014, the Supreme Court ruled against Aereo, finding that Aereo had violated copyrights held by the networks. **The point of contention was whether Aereo's business model constituted a "public performance" rather than merely enabling individual viewing**, and if so, Aereo would be legally required to obtain permission from the copyright owners of any programs it transmits. See Orly Lobel, "The Law of the Platform" Minn. L. Rev. 87 (2016)., P 139-142

[156] Are these digital companies service providers or brokers of individualized exchanges? Should they be viewed as merely enabling intermediaries or robust corporate infrastructures? Ibid. 91

[157] The electronic intermediary service will benefit from the principle of freedom to provide services as guaranteed in EU legislation — Article 56 TFEU and Directives [2006/123] and [2000/31]; b) they cannot be held responsible for any ill-execution of the underlying contract (service) or for damage accruing therefrom under Art. 3 E-Commerce directive; and c) they can claim to be fully absolved from any liability, including for misrepresentation, offensive or illegal content, under Articles 13,14. 15 of the E-Commerce Directive.

[158] The key criteria to be considered are: a) the circumstance that the collaborative platform sets the final price to be paid by the user; b) the fact that the platform sets other key contractual terms; and c) the fact that the platform owns the key assets used to provide the underlying service. See European Commission, A European agenda for the collaborative economy, COM(2016) 356, 6.

market terms,[159] do online platforms provide an information society service and do they also supply an underlying service in the end?[160] If platforms do not provide a merely intermediation service, instead, they provide material services (i.e., transportation, accommodation etc) then, often is required a license and full liability for their provisions towards users.

Indeed, collaborative/sharing platforms such as BlaBlaCar, Uber, StarTaxi and Airbnb have been accused by incumbent market operators for unfair and/or anticompetitive behaviour in the underlying market, that is, to date, especially in the sectors of transport and accommodation. In specific, in the transport sector, there have three important judgments. In Spain, the BlaBlaCar platform, a ridesharing company connecting car owners with potential user for long distance journeys, has been held by the Madrid Commercial Tribunal to be a mere intermediary, not in competition with traditional coach and train service. [161] In EU level the ECJ has, respectively, ruled in 2017 and in 2020 on UberPop and Star Taxi app. In UberPop [162] the Court declared that an intermediation service such as UberPOP must be classified as "a service in the field of transport" within the meaning of EU law – thus not as an information society service.[163] While in the Star Taxi App, (2020)[164] according to the Court, a digital platform which displays available taxis but does not actively match a taxi and a passenger, does not set prices and does not manage payments is providing an information society service services regulated under Directive 2000/31 on electronic commerce.[165]

The Court decides as in Airbnb judgment (2019, C-390/18 AHTOP v. Airbnb

[159] See M Inglese, Regulating the Collaborative Economy in the European Union Digital Single Market (Springer 2019) p. 20.

[160] Any discussion of the legal issues raised by digital platforms faces at the outset two main difficulties. The first is the lack of a clear and widely shared definition of what a digital platform is. The second is the stark het-erogeneity of the issues involved, which are not limited to a single discipline, but lie at the interface of different branches of the legal system, like consumer law, competition law, administrative law, labor law, data protection, etc. Digital platforms have been defined either broadly or narrowly. See G. Resta, "Digital platforms under Italian Law" in U Blaurock (eds) *Plattformen* (Nomos 2018) p. 100; See K Sein "Legal problems of electronic platform economy – Estonian perspective" in U Blaurock (eds) *Plattformen* (Nomos 2018) p. 80;

[161] The Commercial Court in Madrid decided that BlaBlaCar was only mediating in the provision of the carpooling service, and furthermore, that the underlying carpooling services mediated by BlaBlaCar are private services that can be provided with no license as the price is below EUR 0.19/km, the legal reference to reimburse expenses to civil servants when traveling with their own car; that is, the service is being provided with no profit. See, *Confesbus v Blablacar* SJM M 6/2017 (2 February 2017) ES:JMM: 2017:364.

[162] Uber Spain was memorable for introducing a new test for determining whether an online platform provides an information society service caught by the *lex speciali* of the E-commerce Directive or whether it provides a composite service governed by general EU law on the freedom to provide services (or not, if the service relates to transport). Almost two years after Uber decision, the focus of the regulatory battle shifted towards short term rental platforms. See Finck M, "Distinguishing internet platforms from transport services", 55 CMLR (2018) pp. 1619-1640.

[163] Case C-434/15, *Elite Taxi vs. Uber*, EU:C:2017:981.

[164] Start Taxi App, operates a smartphone application that puts taxi service users directly in touch with taxi drivers. The application makes it possible to run a search, and then displays a list of taxi drivers available for a journey. The customer is then free to choose a driver on that list. Star Taxi App does not forward bookings to taxi drivers and does not set the fare, which is paid directly to the driver at the end of the journey.

[165] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereafter "E-Commerce Directive").

Ireland)[166] but against the precedent in Elite Taxi v UberPop.[167] In specific, Uber Spain was memorable for introducing a new test for determining whether an online platform provides an information society service caught by the *lex specialis* of the E-Commerce Directive 2000/31 or whether it provides a composite service governed by general EU law on the freedom to provide services (or not, if the service relates to transport).[168] Unlike in UberPop, in Airbnb and Star Taxi App, the ECJ took a different view which will have some important implications on the debate of how to regulate platform economy in general.[169]

In a nutshell, whether a collaborative platform also provides the underlying service will normally have to be established on a case-by-case basis. As established by the ECJ, several factual and legal criteria can play a role in this regard. The level of control or influence that the collaborative platform exerts over the provider of such services will generally be significant. Additionally, since the predominant arrangement underlying the EU legislation is the chain model of contracts, the triangle structure used by platforms does not make an easy fit. In other words, EU law does not provide a clear answer to the question about the platform's position within contractual relations, and what legal consequences follow from the platform's engagement into the process of concluding (and potentially performing) contracts between customers and suppliers. Therefore, when it comes to the possible scope of legislative intervention, there are three topics that would be relatively easy to introduce and would offer added value to the current legislative environment: (1) clarification of the platforms' status, (2) clarification of the users' status, and (3) regulating reputational systems. Clarification of the platforms' status could improve the transparency of the market and increase users' understanding when it comes to the position of the platform, which fits well with the rationale of the existing *acquis*. A further going legislative action, i.e., introducing the platform's liability, would require a more elaborate, fully fleshed out piece of legislation.[170] Indeed, the EU 2020 Proposal for Digital Services Act (DSA) -

[166] Similar to Elite Taxi, in Airbnb Ireland, an association of real estate brokers based in Paris challenged the fact that Airbnb advertises rental opportunities online without having been duly authorized to do so through a professional card. Its delivery is subject to the fact that an applicant has a demonstrable professional qualification, provide financial guarantees and have professional liability insurance. Of course, Airbnb and, above all, its hosts have none. Airbnb contests that these restrictions are not applicable to the extent that its activities fall within the scope of the E-Commerce Directive. Thus, following - or departing - from the Uber judgement, the CJEU was required to rule on whether Airbnb is a market maker not limited to matching demand and supply, but engaged in offering the underlying service as well. By its judgment of 19 December 2019, the Grand Chamber of the Court held that Airbnb's intermediation service is an information society service regulated under Directive 2000/31 on electronic commerce. See Murati E, (September 2020), Airbnb and Uber: two sides of the same coin (September 2020) available at: http://www.medialaws.eu/airbnb-and-uber-two-sides-of-the-same-coin/ accessed 20 October 2020.

[167] See Curia press release https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-12/cp200149en.pdf accessed 13 December 2020.

[168] See M. Finck, Distinguishing internet platforms from transport services, in CMLR, 55, 2018, 1619 ss

[169] See Murati E, (September 2020), Airbnb and Uber: two sides of the same coin (September 2020) available at: http://www.medialaws.eu/airbnb-and-uber-two-sides-of-the-same-coin/ accessed 20 October 2020

[170] Clarification of the users' status to enhance the way in which platforms function would constitute a targeted, platform-focused action, and would not cause far-reaching changes to the structure of the existing EU regulation. Rules on reputational systems – introduced either as a self-standing act, or as a part of a larger agenda – would trigger an issue of fundamental importance for the digital market. See Aneta Wiewiórowska-Domagalska "Online Platforms: How to Adapt Regulatory Framework to the Digital Age?" EU Parliament (2017) p. 9

amending Directive 2000/31/EC on e-commerce[171] - intends to strengthen the EU single market and clarify digital services' responsibilities and liabilities. In combination to the ECJ suggested parameters, the DSA would provide legal certainty to platform providers and user of these on whether the platform is also offering the underlying service or not. An in-depth analysis of the DSA requires a separate research.

4.2 Exploring regulatory interventions targeted to digital platforms.

In addition to the DSA, on 15 December 2020, the EU Commission has also published a proposal for Digital Markets Act (DMA)[172] which aims to tackle the economic power of large online platforms.[173] This section aim to provide a brief overview of the DMA and of the EU main reasons for proposing it. However, before adopting the DMA proposal, the EU initiative to regulate the platform economy can be dated with the adoption of Regulation (EU) 2019/1150[174] on "promoting fairness and transparency for business users of online intermediation services" (the P2B Regulation), which applies from July 2020 onwards. The increasing dependence of businesses on online platforms to sell their goods and services to consumers has allowed for several harmful trading practices against which no redress was possible. Accordingly, the Regulation aims to restore some balance in the P2B relationships to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. It lays down rules to ensure that business users of digital platforms are granted appropriate transparency, fairness and effective redress possibilities (Art. 1). It addresses several problematic practices by online platforms (Amazon was amongst the main regulatory targets of the EU legislator [175]) and search engines by focusing on high level transparency requirements. These requirements provide clear principles on implementing changes to terms and conditions (hereafter T&C), the grounds for suspension or termination of a platform, ranking parameters and any preferential treatment of a platform's own products or services, and access to personal and other data and the use of most favoured nation (MFN) clauses.

Subsequently, the DMA proposal follows the Communication *Shaping Europe's Digital Future*, which indicated that additional rules may be needed to ensure contestability, fairness and innovation and the possibility of market entry, as well as public interests that go beyond competition or economic considerations. The Proposal establishes *ex ante* rules to ensure that markets characterised by large platforms (ie.e, Google, Amazon, Apple, etc) with

[171] Proposal for a regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending directive 2000/31/EC com(2020) 825 final 2020/0361
[172] Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) Brussels, 15.12.2020; (2020) 842 final 2020/0374 (cod)
[173] See European initiatives to hobble u.s. tech companies (November 10, 2020) the digital services act, the digital markets act, and the new competition tool, accessed 12 December 2020.
[174] Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/59.
[175] See Ducuing Charlotte, Dutkiewicz Lidia, Miadzvetskaya Yuliya (2020) TRUSTS *Trusted Secure Data Sharing Space. D6.2 Legal and Ethical requirements*, p. 59.

significant network effects ("gatekeepers"), remain fair and contestable.[176] The objective of the DMA is to address at EU level the most salient incidences of unfair practices and weak contestability in relation to so-called "core platform services" (Art. 2 (2)). To this end, the Proposal: a) establishes the conditions under which providers of core platform services should be designated as "gatekeepers" (Chapter II); b) sets out the practices of gatekeepers that limit contestability and that are unfair, laying down obligations that the designated gatekeepers should comply with, some of which are susceptible to further specification (Chapter III). For instance, in Art. 6 (d) prohibits self-preferencing practices (i.e., unfair treatment in rankings, differentiation in terms of access to data, etc). This rule is inspired by the decision of the European Commission in June 2017 to fine Google €2.42 billion for abusing its dominance in the market for online search by systematically giving prominent placement to its own comparison-shopping service compared to competing comparison-shopping services.[177] The concept has also featured in other pending proceedings,[178] being the most recent one the case of Spotify vs. Apple. Music streaming app Spotify, for example, has complained that it is being treated unfairly in comparison with Apple's music app because of exorbitant commission fees, self-preferencing, restricted promotions, and limited integration with Apple's broader ecosystem.[179] Indeed, in April 2021, the EU Commission has supported Spotify's claim back in 2019 and has found that Apple has broken EU competition rules (Art. 102 TFEU) with its App Store policies;[180] (b) provides rules for carrying out market investigations (Chapter IV); c) and contains provisions concerning the implementation and enforcement of this Regulation (Chapter V). For further exploration of the DMA, this work suggests some excellent scholars and report which have already published

[176] See EDPS, (10 February 2021) *Opinion 2/2021 on the Proposal for a Digital Markets Act.*

[177] European Commission, decision of June 27, 2017, Case AT.39740.; See Press release (27 June 2017) Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784 accessed 13 May 2021.

[178] Among others, at European level see Cases AT.39740 Google Search (Shopping), June 27, 2017; AT.40462 Amazon, July 17, 2019; at national level see: (i) *Italian cases A528*—Amazon: investigation launched on possible abuse of a dominant position in online marketplaces and logistic services' (Press release, April 16, 2019) https://en.agcm.it/en/media/press-releases/2019/4/Amazon-investigation-launched-on-possibleabuse-of adominant-position-in-online-marketplaces-and-logistic-services; *A529—Google*: investigation launched against Google for alleged abuse of a dominant position' (Press release, May 17, 2019) https://en.agcm.it/en/media/pressreleases/ 2019/5/ICA-investigation- launched-against-Google-for-alleged-abuse-of-a-dominantposition; (ii) *Dutch Apple case* (see ACM press release, ACM launches investigation into abuse of dominance by Apple in its App Store, available at https://www.acm.nl/en/publications/acm-launches-investigation-abuse-dominance-apple-its-app-store.

[179] See For a discussion, see Friso Bostoen, 'Spotify lodges antitrust complaint against Apple: it's "time to play fair" in the music streaming industry' CoRe Blog (24 April 2019) www.lexxion.eu/en/coreblogpost/spotify-apple/ accessed 1 May 2021.

[180] To put in the words of the Executive Vice-President Margrethe Vestager, in charge of competition policy, "*With Apple Music, Apple also competes with music streaming providers. By setting strict rules on the App store that disadvantage competing music streaming services, Apple deprives users of cheaper music streaming choices and distorts competition. This is done by charging high commission fees on each transaction in the App store for rivals and by forbidding them from informing their customers of alternative subscription options*". In these terms, see EU Commission (30 April 2021) *Antitrust: Commission sends Statement of Objections to Apple on App Store rules for music streaming providers*, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061 accessed 30 April 2021.

their preliminary assessment of the proposal.[181]

What the EU is trying to achieve at EU level, Germany has already approved the Tenth Act Amending the Act against Restraints of Competition for Competition Law 4.0 (ARC-Digital Competition Act) by the German Bundestag on 14 January 2021 and came into force on 19 January 2021.[182] The Act is intended to realise the German government's goal of creating a "regulatory framework for digital competition". [183] Some of the key changes are: (1) Companies with paramount cross-market significance. A novel regulatory approach targets a limited number of large "gatekeepers and intermediaries" in digital markets (new Section 19a GWB).

Currently, the *Bundeskartellamt* is examining whether Amazon is of paramount significance for competition across markets; [184] (2) List of conduct considered problematic. The types of conduct of such companies with "paramount cross-market significance" that the Federal Cartel Office may now prohibit under Section 19a (2) GWB includes, among others: a) engaging in self-preferencing when providing access to supply and sales markets (in particular with regard to the display of offers and exclusive pre-installation of offers; b) refusal to provide essential data to competitors; c) impeding the interoperability of products or services or the interoperability of data; (3) New rules on merge controls and cartel investigation. If the DMA would be adopted, the new German law would be surpassed be the new EU rules.

Conclusions.

This research has aimed to provide an analysis of the intersection between digital platforms, economics, and law. It has discovered the following findings. First, as far as digital platforms operate in various economic sectors, their definition is as dynamic as the possibilities for tech companies to reinvent their business digitally or develop new businesses online. Second, the rise of

[181] See Cabral L, *et al.*, (2021) *The EU Digital Markets Act - A Report from a Panel of Economic Experts*, EU Commission; Cerre report (December 2020) *Digital Markets Act: Making economic regulation of platforms fit for the digital age*; Cerre report (January 2021) *The European proposal for a Digital Markets Act: A first assessment*; See Damien Geradin, (May 27, 2021) The DMA proposal: Where do things stand ? available at https://theplatformlaw.blog/2021/05/27/the-dma-proposal-where-do-things-stand/ accessed 2 June 2021.

[182] See Gesetz gegen Wettbewerbsbeschränkungen (GWB) - "Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S. 1750, 3245), das zuletzt durch Artikel 5 Absatz 3 des Gesetzes vom 9. März 2021 (BGBl. I S. 327) geändert worden ist. Available at https://www.gesetze-im-internet.de/gwb/BJNR252110998.html ; For the formal English translation see https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Others/GWB.pdf?__blob=publicationFile&v=7

[183] See Bosch W, et al. (09.02.2021) *The tenth Amendment to the Act Against Restraints of Competition – digital competition act is in force,* available at https://www.gleisslutz.com/en/Digital_Competition_Act_is_in_force.html#:~:text=The%20Amendment%20generally%20strengthens%20the,to%20intervene%20in%20this%20regard Accessed 21 April 2020; See also Herrlinger *et al.,* (20 January 2021) New Competition Law in Germany - 10th amendment to German Act against Restraints of Competition passed, available at https://www.whitecase.com/publications/alert/new-competition-law-germany-10th-amendment-german-act-against-restraints accessed 2 June 2021

[184] See Bundeskartellamt (18 May 2021) Proceedings against Amazon based on new rules for large digital companies (Section 19a GWB), available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/18_05_2021_Amazon_19a.html accessed 18 May 2021.

platform and collaborative economy comes with many benefits to both consumers and business (i.e., platforms reduce search/ transaction costs, build trust, allow consumers to act as 'sellers' or 'workers', increase social capital formation, etc.).[185] Third, almost all digital platforms are characterized by network effects, algorithm management and pricing strategies which drive and increase the volume of transaction on the platforms. Fourth, the diriment role of online platform provider rises specific legal issues in relation to the market operation for each category of digital platforms. Thus, digital platforms have been challenging the law, and this is a key feature and consequence of their operation. They rise regulations concerns in various sectors and dimensions both from a supplier and consumer perspective. Nevertheless, judges, regulators and concerned public authorities are trying to address these challenges either by fitting the platform economy under the existing regulatory framework or by developing sector-specific legal intervention to tackle various competition and consumer issues. Indeed, due to the rise of new business models and digital services, the EU has started to update some of its legal framework fro the internal market. It has been suggested that, before the development of new regulations on online platforms, policymakers must take into account two things: first, they need to consider the underlying characteristics of platforms and business models rather than trying to deal with digital platforms as single category; and, second, they must explore existing instruments and options that can be applied to digital platforms before considering new rules.[186]

Additionally, a future regulatory EU framework for the platform economy should not only address platform operators as market intermediaries, but should also consider their role as actors participating in the regulatory chain, be it as a provider of private ordering services or as a regulatory intermediary implementing public ordering.[187]

Finally, the fact that digital platforms exploit huge quantities of data, including personal data, raises new issues such as data portability, open data, sharing/accessing data, data as commodities, data sovereignty, etc. Accordingly, a key proposal of the new European data strategy document[188] is the creation of nine common EU data spaces across the following sectors: industrial (manufacturing), mobility (transport), health, finance, energy, agriculture, public administration, etc. In specific, such data spaces will facilitate access, pooling and sharing of data from existing and future transport and mobility databases.[189]

---

[185] Eva S. & Bruno B, 2015, "*Online Intermediaries: Impact on the EU economy*", https://www.copenhageneconomics.com/publications/publication/online-intermediaries-impact-on-the-eu-economy. Pg. 46.

[186] See Pieter Nooren et al. "Should We Regulate Digital Platforms? A New Framework for Evaluating Policy Options" in Policy & Internet (2018) p. 266

[187] Increasingly, public authorities are involving platforms in their regulatory activity, drawing on their superior operational capacities and direct access to data and effective means of influencing the behaviour of platform users. In such a scenario, platform providers act as regulatory intermediaries. See Busch, Christoph, "Self-Regulation and Regulatory Intermediation in the Platform Economy" p. 6, (November 30, 2018). Forthcoming in: Marta Cantero Gamito & Hans-Wolfgang Micklitz (eds.) The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes, Edward Elgar 2019. Available at SSRN: https://ssrn.com/abstract=3309293

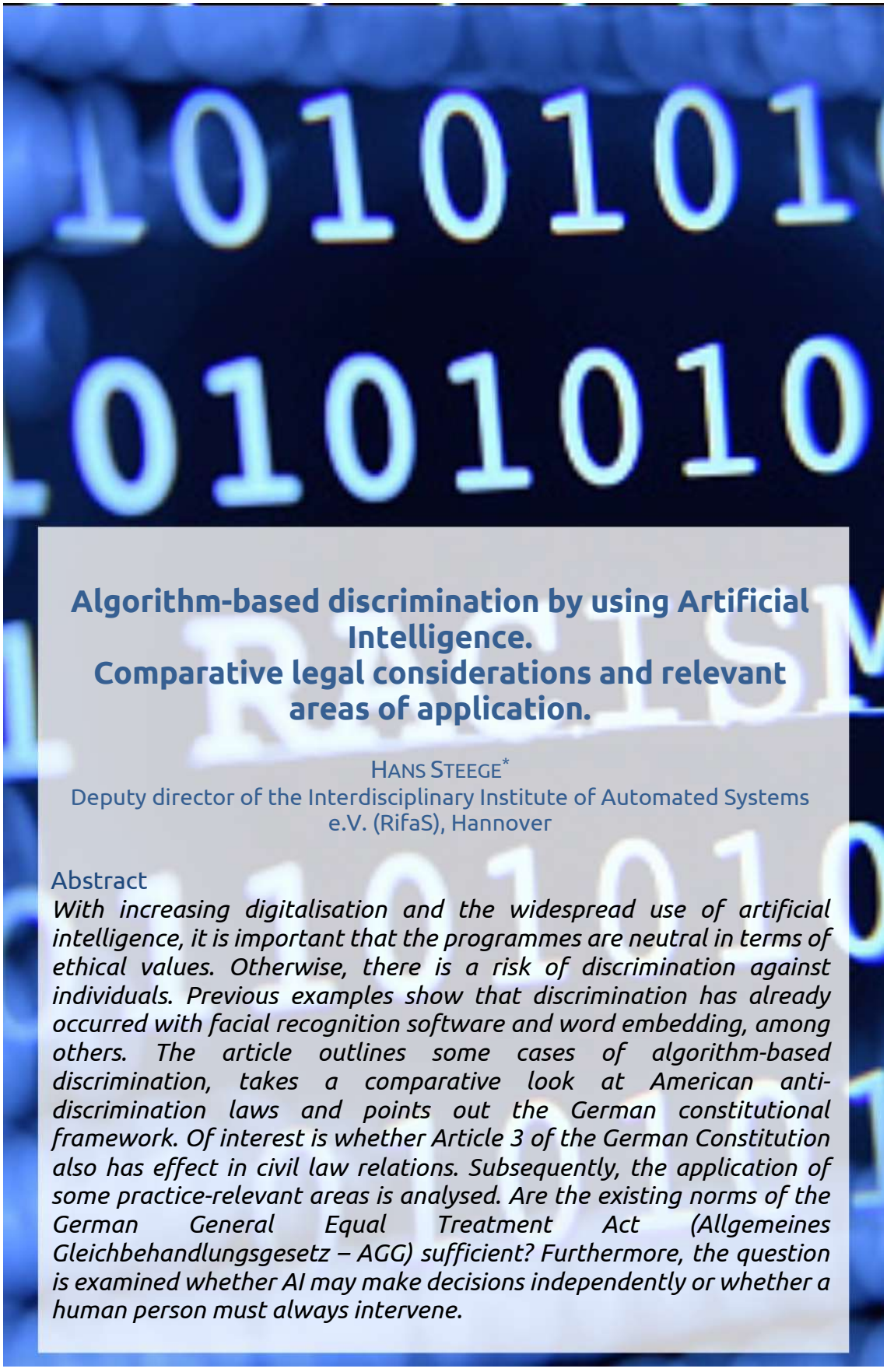
[188] See EU Commission 'A European strategy for data' COM (2020) 66 final, p. 16.

[189] Ibid. p. 22.

The first step towards this goal was the adoption of the Proposal for a Regulation (2020/) on European data governance – an enabling framework for common European data space (Data governance Act).

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012



Algorithm-based discrimination by using Artificial Intelligence. Comparative legal considerations and relevant areas of application.

HANS STEEGE*
Deputy director of the Interdisciplinary Institute of Automated Systems e.V. (RifaS), Hannover

Abstract

With increasing digitalisation and the widespread use of artificial intelligence, it is important that the programmes are neutral in terms of ethical values. Otherwise, there is a risk of discrimination against individuals. Previous examples show that discrimination has already occurred with facial recognition software and word embedding, among others. The article outlines some cases of algorithm-based discrimination, takes a comparative look at American anti-discrimination laws and points out the German constitutional framework. Of interest is whether Article 3 of the German Constitution also has effect in civil law relations. Subsequently, the application of some practice-relevant areas is analysed. Are the existing norms of the German General Equal Treatment Act (Allgemeines Gleichbehandlungsgesetz – AGG) sufficient? Furthermore, the question is examined whether AI may make decisions independently or whether a human person must always intervene.

Keywords: Artificial intelligence; algorithm-based discrimination; constitutional law; GDPR; contract law.

Introduction.

Digitalization is spreading to more and more areas, whether in everyday life or in industry. The interconnection of systems offers numerous new possibilities, first and foremost the exchange of information. In addition, automation promises to make processes simpler. Artificial intelligence (AI) differs significantly from conventional software, which follows an "if-then" scheme and is considered a key technology.

While the source code of rule-based programmes provides information about why a particular decision was made, this is fundamentally different with AI. This circumstance, in combination with autonomous learning, harbours dangers that concern discrimination, among other things. When AI is used on the capital market to act as an investment advisor, to grant loans and flats, to conclude insurance contracts or to make a prognosis about the recidivism of a criminal in court proceedings, sensitive areas of our everyday life and coexistence are affected.

The art of interpreting words and sentences, in short: the correct semantic understanding, poses challenges for AI. While the analogy "man is to king as woman is to x" was solved satisfactorily with “queen“ in one study, the combination "man is to computer programmer as woman is to homemaker" is discriminatory.[1] This reveals problems that do not only concern language and words, but also the understanding of the value of individual persons and groups of persons, as well as prejudices that finally affect everyone who comes into contact with AI.

In the following, after a comparative legal consideration, some areas of application of AI will be examined with regard to possible discrimination, whereby the focus is on labour law. In addition to equal treatment and data protection, competition and antitrust law are also affected, for example when it comes to pricing.[2] However, the latter will not be the subject of this article.

---

[*] The author *Steege* works in the automotive sector and is Deputy director of the Interdisciplinary Institute of Automated Systems e.V. (RifaS). A previous version of this paper was published in German language in the journal *Multimedia und Recht* (MMR) 2019, 715-721. He is grateful to be publishing in this journal to strengthen the research bound between the Research Centre in Private Law (ReCEPL) at University Suor Orsola Benincasa di Napoli and the RifaS in Hanover.

[1] T Bolukbasi/K-W Chang/J Zou/V Saligrama/A Kalai, ‘Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings’, arXiv:1607.06520, 2016, Cornell University, 1 ff.

[2] B Paal, ‘Missbrauchstatbestand und Algorithmic Pricing’ [2019] GRUR, 43 ff.

1. Algorithm-based discrimination.

1.1 Google Photos.

Alongside Flickr,[3] Google Photos[4] in particular has a dominant position in the market. Google's software caused quite a stir when it classified black people as gorillas.[5] Previously, the software identified people, regardless of their skin colour, as dogs.[6] In order to make facial recognition possible, the algorithm has to be provided with a lot of information. The software learns on the basis of examples, whereby the composition of the information or example images has a decisive effect on the result.[7]

1.2 COMPAS.

Another example is the use of the software "Correctional Offender Management Profiling for Alternative Sanctions" (COMPAS). It is used in the United States to predict the probability that a person will commit a crime (again).[8] COMPAS calculates from answers to 137 questions how likely it is that the person in question will commit a crime again or will no longer be conspicuous in terms of criminal law. But why is the software so criticised[9] and should have been the subject of a case before the US Supreme Court in the past?[10] The following two cases and probabilities will illustrate this:

- Brisha Borden (18) tried to steal a bicycle when the opportunity arose. She was convicted of stealing the bicycle worth US-$ 80. COMPAS determined a high risk of recidivism (score 8/10).[11]
- Vernon Prater (41) robbed a shop (loot: US-$ 86.35). He had a previous conviction for armed robbery (score 3/10).
- Borden did not recidivate, Prater, on the other hand, robbed a shop and stole electronic items worth several thousand US dollars and is in prison. Prater is "white" - Borden "black".

The results of COMPAS are used both for the making of judgements, the sentence and for an application for early release. The Justice Department's National Institute of Corrections (NIC) even goes so far as to encourage all those involved in the process to use the software at every moment of the proceedings. [12] It is obvious that the software tends to classify African-Americans as criminals, but whites less often.

The COMPAS example shows that programmes are not neutral. From a constitutional and ethical point of view, it is incompatible with human dignity,

---

[3] https://de.wikipedia.org/wiki/Flickr.
[4] https://de.wikipedia.org/wiki/Google_Fotos.
[5] https://arstechnica.com/information-technology/2015/06/google-dev-apologizes-after-photos-app-tags-black-people-as-gorillas/.
[6] https://twitter.com/yonatanzunger/status/615586630842236928.
[7] I Chen/FD Johansson/D Sontag, 'Why is my classifier discriminatory?', 2018, arXiv preprint.arXiv.
[8] BT – WD 8-3000-031/17, p. 6.
[9] https://www.nytimes.com/2017/06/13/opinion/how-computers-are-harming-criminal-justice.html.
[10] Loomis v. Wisconsin, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017).
[11] *ProPublica*, available at: https://www.propublica.org/article/machine-biasrisk-assessments-in-criminal-sentencing.
[12] ibid.

the principle of the rule of law and the right to a fair trial that such software is used in proceedings in Germany.

2. Description of AI.

Algorithms that follow an "if-then" scheme make their decisions within the framework of what is given. Only what has been specified by the programmer can subsequently be processed by the programme. AI does not only learn on its own, but also uses neural networks and can further develop the previous algorithms. AI is characterised by the fact that information from the outside world can also be processed without prior programming and that corresponding feedback is given.[13] This triad of perception, thinking and acting is the advantage compared to conventional "if-then" codes.[14]

If AI is used in combination, e.g. in an autonomous vehicle, the integrated sensors are crucial for the input quality and have an effect on the process of thinking and the later acting.[15]

The advantage of a missing "if-then-scheme" is at the same time the weakness of AI. It remains open whether decisions can be traced ex post and which parameters were the basis for the decision.

3. Discrimination in the USA.

The debate around discrimination is much more pronounced in the United States, so it is worth looking at the understanding of discrimination there in addition to the legal framework of anti-discrimination laws.

3.1 14th Amendment.

In the USA, paragraph 1 of the 14th Amendment prohibits discrimination: *„All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."*[16]

The statement "No state shall ... deny to any person within its jurisdiction the equal protection of the laws"[17] gives rise to the constitutional requirement of equal treatment of all persons. The 14th Amendment was particularly decisive in cases of discrimination against African-Americans and became significant in the debate on the constitutionality of affirmative actions.[18]

---

[13] H Hexmoor, *Essential Principles for Autonomous Robotics* (Morgan & Claypool Publishers 2013) 25.
[14] H Steege, 'Autonomes Fahren und die staatliche Durchsetzung des Verbots der Rechtswidrigkeit' [2019] NZV, 459, 465; Hexmoor, *Essential Principles for Autonomous Robotics* (n 14) 25.
[15] On this and on possible sources of error in detail Steege, 'Autonomes Fahren und die staatliche Durchsetzung des Verbots der Rechtswidrigkeit' (n 15) 459, 461 f.
[16] https://www.law.cornell.edu/constitution/amendmentxiv.
[17] Known as the „Equal Protection Clause".
[18] Regents of Univ. of California v. Bakke, 438 U.S. 265 (1978).

Constitutionally disputed and from a dogmatic point of view interesting is the consideration whether the Equal Protection Clause can contain two competing protective purposes, namely the "any person line" and the "race line". Thus, the scope of protection of the "any person line" includes every human being. However, the Equal Protection Clause cannot be understood as a commandment of complete equal treatment, which would make any distinction in favour of minorities per se unconstitutional. It is therefore questionable whether the so-called "racial preference" is to be seen merely as a restrictive exception to the principle of "race-neutral equality", or whether an additional area of protection exists that encompasses persons belonging to a minority and which occurs alongside the right to full equal treatment. If one assumes such a scope of protection, the question arises whether both purposes of protection are equally weighted or whether the "race line" takes precedence.[19]

In addition to the constitutional protection, there exists with Title VI Sec. 601 of the Civil Rights Act of 1964 a non constitutional regulation that relates to public institutions: *„No person in the United States shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance."*[20] In addition, there are further anti-discrimination laws in the USA.[21]

3.2. Different types of discrimination.

In the USA, a distinction is drawn between different forms of discrimination:

- (a) Intentional, direct discrimination: The booking software of a restaurant does not allow members of a minority group to reserve a table, regardless of whether the customers can pay or not.
- (b) Non-intentional, direct discrimination: The AI used in a job application process of a craft company does not hire women because they do not appear to be physically strong enough. This type of discrimination is called rational discrimination because it is assumed that there is a correlation between the criterion of belonging to a certain group and a characteristic. In this case, it would be the assumption that women are not physically fit to work in a craft profession.
- (c) Intentional, non-direct discrimination: The AI of a security company only hires people with a certain height, knowing that male applicants have an advantage.
- (d) Non-intentional, non-direct discrimination: A company's software performs special orthography tests during the hiring process because it is assumed that this is a prerequisite for the vacant position. This puts groups at a disadvantage who did not receive an equivalent school education due to external circumstances.

[19] In detail U Beyerlin, '"Umgekehrte Rassendiskriminierung" und Gleichbehandlungsgebot in der amerikanischen Verfassungsrechtsprechung. Zum Bakke-Urteil des U.S. Supreme Court vom 28. Juni 1978" '[1979] ZaöRV, 496 ff.
[20] Available at: https://www.justice.gov/crt/fcs/TitleVI-Overview.
[21] Cf. Title VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000E, 2003; Age Discrimination in Employment Act of 1967, 29 U.S.C. 621-34; Fair Housing Act und Fair Housing Amendments Act, 42 U.S.C. §§ 3601-19.

Having this in mind, what exactly now is discrimination?

A common view is that discrimination occurs when persons are disadvantaged on the basis of irrelevant characteristics (extraneous traits). Thus, anti-discrimination laws are supposed to give everyone the right to freely decide on his or her worth.[22] This is called "deliberative freedoms", according to which everyone can decide for him- or herself how to live without being prevented from doing so by irrelevant characteristics. [23] Irrelevant characteristics are said to be present, whether *chosen* or *given*. Based on a normative understanding, race and age are not self-selected, religion freely chosen and other factors may be due to a past choice.[24] This understanding of anti-discrimination laws - the holding of a number of rights in the form of deliberative freedoms - is unfamiliar in Germany. From a constitutional law dogmatic point of view, the approach of always countering discrimination with the creation of constitutional principles and rights appears difficult.[25]

3.3 Affirmative Actions.

Since unequal treatment by software cannot only occur due to discrimination, the legitimacy of the so-called "affirmative actions" shall be shown. In the past, mainly white people have filed lawsuits against affirmative actions, with the explanation that they have become victims of discrimination because the measures would favour members of minorities. Positive discrimination is mainly justified by the following triology: "correction of bias in standardised tests, compensation for past mistakes and promotion of diversity". [26] Diversity is seen as an argument for the common good. The compensation argument is highly controversial. Critics stress that the current beneficiaries did not necessarily have to suffer and that those at whose expense these measures are taken need not have committed the mistakes.[27] It is also crucial how moral obligations come about. Only then can be answered whether society has such a duty.

If AI is used in the future, e.g. to carry out admission procedures at universities instead of a human being, the same applies here as under the current law. However, it becomes problematic if the reasons for the decision and the underlying criteria are not transparent, i.e. the AI is no longer understandable in retrospect or during the process.

4. (Anti)Discrimination in Germany.

4.1 Constitutional protection.

In Germany, Article 3 (1) of the Constitutional Law (GG) postulates that all

[22] S Moreau, 'What is Discrimination?' (2010) 38 (2) Philosophy & Public Affairs, 143, 147.
[23] ibid 143, 150.
[24] In detail with regard to this concept of the *deliberative freedoms* see *Moreau,* ibid 143, 150.
[25] Other opinion D Hellman, 'Equality and Unconstitutional Discrimination', in D Hellman/S Moreau (eds.), *Philosophical Foundations of Discrimination Law,* (Oxford University Press 2013), 50, 60 ff.
[26] MJ Sandel, *Gerechtigkeit*, (Ullstein Verlag 2013), 230 ff.
[27] ibid, 232.

persons are equal before the law. Paragraph 3 standardises characteristics on the basis of which unequal treatment is prohibited. Although not explicitly mentioned, skin colour is covered by the differentiating characteristic of race due to historical understanding.[28]

a) Predictive policing

Of constitutional interest is the so-called predictive policing, where algorithms make predictions, for example for future crimes, criminals or crime scenes, both preventively and repressively. [29] By evaluating corresponding data, risk profiles are created for individual persons. [30] In addition, the probability of whether a person will recidivate is calculated.[31] Currently, no personal data is used in Germany, so there is no encroachment on fundamental rights.[32] The constitutional hurdles for predictive policing using personal data are very high in Germany.[33] Especially because of the serious infringement and the fundamental rights affected by it, the ultimate decision-making power cannot be shifted to such applications or to an AI. From a constitutional point of view, it follows that the decision-making power must necessarily remain with a human being as long as programmes are not value-neutral, as otherwise the individual is degraded to an object. In addition, it is open how the decision-making process of such an application is designed and how which aspects affect the calculation of probability. As long as this is not transparent, such an algorithm raises constitutional concerns.

b) Art. 3 Basic Law for the Federal Republic of Germany (GG) in civil law relations

Nowadays, programmes make more and more decisions that have a direct impact on individuals. Discrimination can be based on input of data, prejudices or unintended correlations.[34] Economic sectors affected include credit scoring, e-commerce pricing and automated job recruitment processes. [35] The information to be transmitted in each case can lead to different evaluations, whereby, for example, the place of residence can be decisive.[36] For example, a certain nationality can be inferred from a city district. Other data - possibly not queried - can also correlate with each other, resulting in intentional, non-direct discrimination that is impossible or difficult to prove. The respective source codes would have to be disclosed in a legal procedure, which, however, is not to be assumed.

---

[28] EGMR, U. v. 13.12.2005, App.No. 55762/00 und 55974 (Timishev gegen Russland), Ziff. 55.
[29] I Härtel, 'Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren' [2019] LKV, 49, 54; S Egbert, 'Siegeszug der Algorithmen? Predictive Policing im deutschsprachigen Raum' [2017] APuZ 32-33, 17, 19; T Knobloch, 'Vor die Lage kommen: Predictive Policing in Deutschland' [2018] Stiftung Neue Verantwortung/Bertelsmann Stiftung, 8.
[30] AG Ferguson, 'Policing Predictive Policing' [2017] Wash. U. L. Rev., 1112, 1142 ff.
[31] T Rademacher, 'Predictive Policing im deutschen Polizeirecht' [2017] AöR, 366, 370.
[32] Härtel, 'Digitalisierung im Lichte des Verfassungsrechts' (n 30) 49, 54; Knobloch, 'Predictive Policing in Deutschland' (n 30) 5.
[33] In this direction T Singelnstein, 'Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention' [2018] NStZ, 1, 8.
[34] So also T Wischmeyer, 'Regulierung intelligenter Systeme' [2018] AöR, 1, 26 ff.
[35] M Martini, 'Algorithmen als Herausforderung für die Rechtsordnung' [2017] JZ, 1017, 1018.
[36] ibid 1017, 1018; Härtel, 'Digitalisierung im Lichte des Verfassungsrechts' (n 30) 49, 56.

In order for those affected to be able to refer to Article 3 of the Constitutional Law, it would have to have indirect third-party effect. For a long time, however, the Bundesverfassungsgericht (German Federal Constitutional Court, short: BVerfG) rejected this in the case of Article 3 (1) and (3) of the GG (German Constitutional Law).[37] The BVerfG´s most recent judgment on Article 3 (1) GG recognises an indirect third-party effect in the relationship between private parties for special constellations: If a private party uses its monopoly or structural superiority to exclude persons from "participation in social life" without an objective reason, the necessary preconditions are met.[38] Whether the use of AI establishes structural superiority depends on the individual case.[39]

4.2 General Equal Treatment Act (AGG).

The non constitutional specification is found in the norms of the AGG, which are based on EU law.[40]

The General Part of the AGG specifies the objective of the law. § 1 contains the characteristics according to which no unequal treatment may take place. The prohibited grounds include race, ethnic origin, gender, religion, ideology, disability, age and sexual identity. § 2 standardizes the scope of application, § 3 the definitions. § 4 regulates the case of unequal treatment on several grounds. § 5 deals with affirmative actions.

Chapter 2 of the AGG determines the protection of employees against discrimination, chapter 3 the protection against discrimination in general civil law relations, whereby not all areas are covered. In further chapters the AGG deals among other things with the regulations for legal protection. The latter, however, will not be the focus of this paper.

a) Aim of the AGG

The aim of the Act is to prevent and eliminate discrimination.[41] This is to be taken into account in the interpretation of the norms of the AGG under the aspect of effective protection[42] and takes into account the "effet utile" of the European blueprint.[43]

b) Forms of discrimination

The AGG distinguishes in § 3 between direct discrimination (para. 1) and indirect discrimination (para. 2). Direct discrimination occurs when a person is treated disadvantageously in comparison to another person in a comparable situation on the basis of one of the grounds normed in § 1. Leaving aside Art. 22 of the GDPR, it can be assumed that in the case of a

[37] Härtel, 'Digitalisierung im Lichte des Verfassungsrechts' (n 30) 49, 57; M Jestaedt, 'Diskriminierungsschutz und Privatautonomie' (2005) 64 VVDStRL, 298, 340f.; G Britz, 'Diskriminierungsschutz und Privatautonomie' (2005) 64 VVDStRL, 355, 361f.

[38] BVerfG, B. v. 11.4.2018 – 1 BvR 3080/09, marg. no. 41; in detail BeckOK GG/*Kischel*, 47th edn, Status: 15.5.2021, Art. 3 marg. no. 93-93b.

[39] Examples can be found in Härtel, 'Digitalisierung im Lichte des Verfassungsrechts' (n 30) 49, 57.

[40] Compare RL 2000/43/EG; RL 2000/78/EG; RL 2002/73/EG; RL 2004/113/EG.

[41] On the individual characteristics of discrimination *Thüsing*, in: MüKoBGB, 8th edn 2018, § 1 AGG marg. no. 15 ff.

[42] Staudinger/*Serr*, BGB, Vol. 2, 17th edn, § 1 marg. no. 1.

[43] *EuGH* Slg. 1960, 683, 708; 1979, 1629.

decision by AI, without the intervention of a human being, the output of the AI is a treatment in the sense of § 3 (1) of the AGG, so that the requirement of a human act or omission [44] should be reconsidered legislatively. Otherwise, algorithm-based discrimination would not be a treatment in the sense of § 3 (1) AGG.[45] Discrimination can occur both by active doing and by omission.[46]

Indirect discrimination occurs when rules, criteria or procedures that appear neutral at first sight discriminate against persons on the basis of one of the grounds listed in § 1 AGG. However, this can be justified if there is a legitimate aim and the means are appropriate and necessary. However, justification must already be examined as a negative element of the offence. [47] If the discrimination is lawful, the element of the offence is already not fulfilled, so that it does not result in the element of the offence being given and the unlawfulness being lacking.[48] In practice, this has no effect.[49]

Indirect discrimination is more difficult to prove and dogmatically there are doubts about this form of discrimination in this country.[50]

It can be both intentional and accidental: An unintentional indirect bias occurs, for example, when an employer uses a criterion in the application process that is correctly or incorrectly considered relevant and correlates with an irrelevant group membership. However, such a correlation was not intended at any time. If the criterion is lawful, the indirect discrimination can be justified.

Indirect discrimination is intentional if a relevant or irrelevant criterion is used in the knowledge that it correlates with an irrelevant group membership, although it is precisely this group that should be covered.

c) Affirmative actions (positive discrimination)

In § 5, the AGG refers to positive discrimination, which must be appropriate and reasonable and prevent or compensate for existing disadvantages due to a reason mentioned in §1 AGG.

Positive discrimination differs from reverse discrimination in its objective and justification. It is not clear whether time is a factor in the legitimacy of positive discrimination.

Affirmative action disadvantages individuals in order to reverse or counteract the disadvantage of others; it is thus justice for one and injustice for the other.[51] Two views are held in Germany on the solution to this moral dilemma: On the one hand, there is already no discrimination terminologically, but a permissible positive action. [52] On the other hand, there is discrimination in fact, but this is justified because positive action is a

[44] BeckOK ArbR/*Roloff*, 60th edn, Status: 1.6.2021, AGG § 3 marg. no. 2.
[45] K v. Lewinski/R de Barros Fritz, 'Arbeitgeberhaftung nach dem AGG infolge des Einsatzes von Algorithmen bei Personalentscheidungen' [2018] NZA, 620, 621.
[46] BT-Drs. 17/1780, p. 29.
[47] BT-Drs. 16/1780, p. 33; *BAG* NZA 2010, 222; Roloff (n 45), marg. no. 18.
[48] BT-Drs. 16/1780, p. 32.
[49] Roloff (n 45), marg. no. 18.
[50] Thüsing (n 42), marg. no. 24.
[51] R Alexy, *Theorie der Grundrechte* (Suhrkamp Verlag 1994) 78 f.
[52] *Schiek/Schiek*, AGG, 2007, § 5 marg. no. 3; Erman/*Armbrüster*, BGB, Vol. I, 15th edn, AGG § 5 marg. no. 1.

corresponding justification.[53] The second view is to be followed for dogmatic and factual reasons; after all, there can be no positive discrimination that does not discriminate. Positive action can at most justify the disadvantage it creates, but it is ultimately discrimination.

5. Relevant areas of application.

Due to the particular practical importance, the following will deal with employment relationships, tenancy law, administrative law, court proceedings, lending and investment advice.

5.1 Employment law.

The use of AI generally promises an increase in objectivity, whether in the job application process or in preventive measures to prevent criminal offences in companies. For example, personality analyses are produced by AI.[54] At first glance, it seems that AI is free of bias.[55]

a) Recruitment

AI is increasingly used in job application processes.[56] Objectivity and the reduced time required are cited as positive factors.

The possibility of discrimination in these procedures by AI has hardly been considered so far.[57] In addition to erroneous or undetected correlations, prejudices make the software susceptible to discriminating against applicants, for example when words are linked to certain associations, as in the example above. Following the sentence "man is to computer programmer ...",[58] an algorithm would favour men and consider women unsuitable when hiring a programmer.

The use of personality tests in online applications increases the risk of discrimination on the grounds of disability and is also a violation of the AGG.[59] If personality profiles are created in the application process by using language analysis software, as is often the case in large companies,[60] there

[53] *Calliess/Ruffert/Krebber*, EUV/AEUV, 5th edn 2016, AEUV Art. 157 marg. no. 74; *EuGH* NZA 2010, 1281.
[54] B Dzida, 'Big Data im Arbeitsrecht' [2017] NZA, 541, 542; L Rudkowski, ' "Predictive policing" am Arbeitsplatz' [2019] NZA, 72; C Freyler, 'Robot-Recruiting, Künstliche Intelligenz und das Antidiskriminierungsrecht' [2020] NZA, 284, 287.
[55] See on cognitive biases TS Gendler, 'On the epistemic costs of implicit bias' [2011] Philosophical Studies, 33 ff.
[56] I Wildhaber, 'Die Roboter kommen – Konsequenzen für Arbeit und Arbeitsrecht' [2016] ZSR, 315, 337 ff.; B Dzida/N Groh, 'Diskriminierung nach dem AGG beim Einsatz von Algorithmen im Bewerbungsverfahren' [2018] NJW, 1917.
[57] Dzida/Groh, 'Diskriminierung nach dem AGG beim Einsatz von Algorithmen im Bewerbungsverfahren' (n 57) 1917; M Lützeler/D Kopp, 'Bewerbermanagement-Tools' [2015] ArbRAktuell, 491, 492; A Raif/M Swidersky, 'Typische Fehler in der digitalen Arbeitswelt vermeiden' [2017] GWR, 351, 352; S Mätzig, 'Erfolgsfaktor Anonymität? – Eine rechtliche Einordnung anonymisierter Personalauswahlverfahren' [2017] RdA, 185.
[58] Bolukbasi/Chang/Zou/Saligrama/Kalai, 'Man is to Computer Programmer as Woman is to Homemaker?' (n 2).
[59] Dzida/Groh, 'Diskriminierung nach dem AGG beim Einsatz von Algorithmen im Bewerbungsverfahren' (n 57) 1917, 1918.
[60] K Hummel, Deine Sprache verrät dich, in: FAZ v. 20.5.2015.

is an increased likelihood of being disadvantaged for non-native speakers or persons with a language disability.[61]

b) Predictive policing

In addition, employers may find it advantageous to carry out so-called predictive policing. Here it is particularly interesting whether this is compatible with the GDPR, whether the works council has to agree, whether it is scoring and whether § 31 of the German Federal Data Protection Act (BDSG) applies.

Predictive policing can be used to calculate the probability that an employee will commit a criminal offence against the employer's assets.[62] Predictive policing should not be inadmissible per se despite the not only insignificant encroachment on the general right of personality. Rather, it depends on the limits of data protection.[63] Whether this is the only fundamental right affected seems questionable; after all, the individual becomes a mere variable within a probability calculation, has no insight into the respective parameters and their weighting, and cannot be sure that he or she is not exposed to discrimination.[64]

- *Consent to predictive policing according to § 26 (2) BDSG*
  Predictive policing is lawful from a data protection perspective if the framework of § 26 BDSG is not exceeded.[65] When processing personal data[66] (Art. 4 No. 1 GDPR), the consent of the data subject is ruled out unless it is given voluntarily. However, § 26 (2) BDSG does not per se assume that voluntary consent of an employee never exists.[67] This view cannot be inferred from the wording either. Moreover, the fact that the element of voluntariness must be thoroughly checked is not arbitrary, but follows from the level of protection. If there are reasons to believe that there is a lack of voluntariness, the exact circumstances of the individual case must be considered. In terms of legal policy, there are efforts by the EU Commission and the Art. 29 Data Protection Working Group to negate the element of voluntariness in an employment relationship.[68] In addition, it cannot be assumed that employees will revoke their consent once it has been given without difficulty.

- *Predictive policing on the legal ground of § 26 (1) sentences 1 and 2 BDSG*
  If consent is not possible, § 26 (1) sentences 1 and 2 BDSG can be

[61] Dzida/Groh, 'Diskriminierung nach dem AGG beim Einsatz von Algorithmen im Bewerbungsverfahren' (n 57) 1917, 1918.
[62] W Hentrich/A Pyrcek, 'Compliance und Fraud Monitoring im Zeitalter von digitaler Transformation und Big Data' [2016] BB, 1451, 1452.
[63] Rudkowski, '"Predictive policing" am Arbeitsplatz' (n 55) 72, 73.
[64] Other opinion Rudkowski, '"Predictive policing" am Arbeitsplatz' (n 55) 72, 73.
[65] T Niklas/Thurn, 'Arbeitswelt 4.0 – Big Data im Betrieb' [2017] BB, 1589, 1590.
[66] H Steege, 'Ist die DS-GVO zeitgemäß für das autonome Fahren? Datenschutzrechtliche Aspekte der Entwicklung, Erprobung und Nutzung automatisierter und autonomer Fahrzeuge' [2019] MMR, 509.
[67] Other opinion Rudkowski, '"Predictive policing" am Arbeitsplatz' (n 55) 72, 73.
[68] Cf. BeckOK DatenschutzR/*Riesenhuber*, 36th edn, Status: 1.2.2021, BDSG § 26 marg. no. 43.1 with further references.

considered as an element of permission.Whether § 26 (1) sentence 1 or sentence 2 BDSG applies depends largely on the objective pursued: § 26 (1) sentence 2 BDSG is relevant if the measure serves repressive purposes. [69] This is not (yet) the case with predictive policing. However, only criminal offences are covered, not administrative offences and breaches of contract, no matter how serious they were.[70]

For preventive purposes and to clarify breaches of duty that are not possible under sentence 2, sentence 1 applies. In this respect, sentence 2 does not have any blocking effect.[71]

- *Limits of predictive policing (GDPR and the German Constitution)*

  Predictive policing finds its limits in the provisions of the BDSG, the GDPR and the GG. There is no limitation of the predictive decision by what is possible for a human mind of the superior in the respective situation of the individual case.[72]

  When such software is used, there must be no total monitoring of the employees, otherwise they will be degraded to an object. The thereby associated encroachment on the general right of personality under Art. 2 para. 1 in conjunction with Art. 1 para. 1 of the German Constitutional Law (GG) cannot be justified. [73] An atmosphere of constant surveillance pressure is inadmissible.[74]

  Article 22 (1) of the GDPR norms that people may not become mere objects based on decisions made by software.[75] Predictive policing does not violate this if a human intervenes between the process of assessment and decision or ultimately makes the decision and the AI merely takes over the assessment/prediction. In this respect, the human being is responsible for checking the correctness and plausibility. [76] It is necessary that the person has sufficient qualifications and media competence.[77] This includes, among other things, a detailed initial introduction to the programme and ongoing training.

  Whether turning away from the principle standardised in Article 22 (1) of the GDPR is constitutionally permissible appears doubtful. If one leaves employment law when considering this principle and takes a look at other areas, such as court proceedings or administrative law, and the question that arises there as to whether

[69] Erfurter Komm. zum Arbeitsrecht/*Franzen*, 21st edn 2021, BDSG § 26 marg. no. 36.
[70] *Franzen* (n 70) marg. no. 37.
[71] *BAG* NZA 2017, 1179 marg. no. 27 ff.; other opinion *LAG Baden-Würtemberg* ZD 2017, 88.
[72] Rudkowski, ' "Predictive policing" am Arbeitsplatz' (n 55) 72, 74; other opinion W Däubler, *Gläserne Belegschaften* (6th edn, Bund-Verlag 2015) marg. no. 120.
[73] Rudkowski, ' "Predictive policing" am Arbeitsplatz' (n 55) 72, 74.
[74] *BAG* NZA 2017, 1205, 1211; *BAG* NZA 2004, 1278, 1281.
[75] K v. Lewinski, 'Überwachung, Datenschutz und die Zukunft des Informationsrechts', in Telemedicus e.V. (ed.), *Überwachung und Recht*, 2014, 1, 16; BeckOK DatenschutzR/*v. Lewinski*, 36th edn, Status: 1.5.2021, DS-GVO Art. 22 marg. no. 2.
[76] BeckOK DatenschutzR/*v. Lewinski* (n 76), marg. no. 23.
[77] S J Golla, 'Abgenickt von Algorithmik – Aktuelles zum Verbot automatisierter Entscheidungen' [2014] PinG, 61, 64.

a decision is issued or not, central principles and fundamental rights speak in favour of not allowing the AI to have the final decision-making power over a human being.[78]

c) Termination

Ultimately, the question arises as to whether a termination of the employment relationship can be made by AI or whether it must be carried out by a human being. If the latter is the case, the termination cannot be based on predictive policing alone, as further preconditions for a termination must be there.[79] The same applies to a dismissal based on suspicion, as the decision of the programme is merely a calculated probability and the further requirements for such a decision must be fulfilled.[80]

In addition, the termination is the most serious interference on the basis of which the employment relationship is ended, so that it seems questionable that the AI may issue a termination without the involvement of a human being (regardless Art. 22 GDPR).

d) Considerations

The final decision must not be left to the software. In addition, the parameters on which the decision or prognosis is based, and their prioritization, must at least be obvious to the intervening human being. Otherwise, he cannot base his decision on the software. This can then at most be a vague point of reference. Moreover, the possibility of discrimination must be completely impossible. Besides, employees must receive extensive initial training and continuous education. Furthermore, the effectiveness and accuracy of the application must be checked at regular intervals.

5.2 Some further areas of application.

In terms of tenancy law, the main question is whether termination may be done by the AI. If a legal regulation such as Art. 22 of the GDPR does not exist, termination by the AI could be considered. However, a distinction must be made between commercial and residential tenancies. In particular, residential tenancies are in a state of tension with regard to the landlord's duty of tolerance towards the tenant.[81] In view of the particularly protected residential space, termination by AI appears problematic. It must be considered whether the use of AI in this area is covered by private autonomy or whether a human being has to decide on the termination of a tenancy agreement for residential space. The allocation of housing by AI, on the other hand, is not problematic, since this is the first step in establishing a contractual relationship. It remains

[78] Other opinion S Meyer, 'Künstliche Intelligenz und die Rolle des Rechts für Innovation' [2018] ZRP, 233, 237.
[79] Rudkowski, ' "Predictive policing" am Arbeitsplatz' (n 55) 72, 77.
[80] In detail ErfK/*Niemann* (n 70), BGB § 626 marg. no. 173-184.
[81] BH Oppermann/H Steege, 'Zur Duldungsproblematik bei der Ausstattung einer Wohnung mit Rauchwarnmeldern; zugleich eine Anmerkung zu BGH, VIII ZR 216/14, VIII ZR 290/14' [2016] WuM, 3 ff.; BH Oppermann/H Steege, 'Duldungspflichten des Mieters – eine zivilrechtliche Analyse' [2017] WuM, 361 ff.

to be seen to what extent the regulations on agency can be applied to AIs and whether the current legal framework is sufficient to answer these and other considerations, e.g. who is actually the contracting party.[82]

In the administration, the use of AI is imaginable in the area of communication with citizens, for example to provide information, as a basis for decisions or as a decision-maker in administrative acts. Whether and to what extent the use of AI is legally possible will not be discussed further here.[83]

AI does not stop at the advocacy sector either. The first judgements dealing with legal tech have already been made. Whether AI can replace a judge remains to be seen.[84] The associated fundamental rights dimension is also a matter for debate, even if it can be assumed that such use is not compatible with the GG for various reasons, there is also the danger here that discrimination can and will occur. Whether in criminal law or in the area of civil law, for example when it is a question of the credibility of a witness statement, prejudices against one gender, against nationalities would also have a massive effect here and thus leave the framework of the due process of law.

Algorithms are also finding their way into banking law, e.g. in so-called robo advisory, and are automating investment advice (§ 1 (1a) sentence 2 no. 1a Banking Act (Kreditwesengesetz – KWG), § 2 (8) no. 10 Securities Trading Act (Wertpapierhandelsgesetz – WpHG) and management (§ 1 (1a) sentence 2 no. 3 KWG, § 2 (8) no. 7 WpHG). It is not only possible to discriminate against consumers through robo advisory by means of algorithms, this also happens in the granting of loans. In individual cases, robo advisory can also be an investment brokerage (§ 1 (1a) sentence 2 no. 1 KWG, § 2 (8) no. 4 WpHG), so that a distinction must be made between civil and supervisory law.

Due to the high potential for disadvantage with regard to the interest and collateral accruing as well as the "whether" of concluding a loan, the use of algorithms should not take place unreflectively here either. Particularly in the case of creditworthiness checks according to §§ 505a, 505b German Civil Code (Bürgerliches Gesetzbuch – BGB), § 18a Banking Act (KWG), there is the possibility of correlation and a resulting disadvantage of certain groups. The limits of automation here are also § 31 Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) as well as Art. 22 GDPR and the special § 10 para. 2 sentence 1 no. 1 Banking Act (KWG).

Robo advisory has so far preoccupied the jurisprudence from the perspective of supervisory law.[85] However, little attention has been paid to the potential for discrimination.[86] Before a loan can be granted, the lending banks must

[82] In detail L Specht/S Herold, 'Roboter als Vertragspartner?' [2018] MMR, 40 ff.
[83] To this M Martini/D Nink, 'Subsumtionsautomaten ante portas? – Zu den Grenzen der Automatisierung in verwaltungsrechtlichen (Rechtsbehelfs-)Verfahren' [2018] DVBl, 1128 ff.; L Guggenberger, 'Einsatz künstlicher Intelligenz in der Verwaltung' [2019] NVwZ, 844 ff.
[84] *LG Berlin* NJW 2018, 2901 = MMR 2018, 848 (Ls.); cf. furthermore on digitalisation of the justice A Paschke, 'Digitale Gerichtsöffentlichkeit und Determinierungsgesamtrechnung' [2019] MMR, 563.
[85] C Baumanns, 'FinTechs als Anlageberater? Die aufsichtsrechtliche Einordnung von Robo-Advisory' [2016] BKR, 366; S Scholz-Fröhling, 'FinTechs und die bankenaufsichtsrechtlichen Lizenzpflichten' [2017] BKR, 133; D Krimphove/K Rohwetter, 'Regulatory Sandbox – Sandkastenspiele auch für Deutschland? [2018] BKR, 494; F Möslein/A Lordt, 'Rechtsfragen des Robo-Advice' [2017] ZIP, 793; *Bitter*, in: Hoeren/Sieber/Holznagel (eds.), Hdb. Multimedia-Recht, 56. EL Februar 2021, marg. no. 59 ff.
[86] See on possible dangers the *BaFin* study, Big Data trifft auf künstliche Intelligenz, 2018, available at: https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html; Martini, JZ 2017, 1017, 1018.

make a prognosis about the probability of contract fulfilment, and this prognosis must be positive, § 505a para. 1 BGB. § 505a (1) BGB contains a legal definition of the creditworthiness test, according to which it depends on the probability of whether "the borrower will fulfil his obligations in connection with the loan contract in accordance with the contract". § 2 (1) sentence 2 Regulation Establishing Guidelines on the Criteria and Methods of Creditworthiness Assessment for Real Estate Consumer Loan Agreements (Verordnung zur Festlegung von Leitlinien zu den Kriterien und Methoden der Kreditwürdigkeitsprüfung bei Immobiliar-Verbraucherdarlehensverträgen – ImmoKWPLV) also requires that it is a reasonably justifiable prognosis and § 3 (1) ImmoKWPLV adds that the borrower's future developments must be included.[87]

In practice, scoring in particular occupies a particularly important area of the creditworthiness check. In addition to possible correlations and effects of place of residence or gender, word embedding also causes problems here. Prejudices are not always easy to identify here, depend on the data that is initially available and primarily arise from biases in the data that is evaluated.[88] Banks and financial service providers must take all this into account when implementing algorithms and robo advisory.

6. Regulation of algorithms.

Due to the risk of discrimination in the use of algorithms and AI, it seems worthwhile to think about a regulation of algorithms that goes beyond the approach of the Article 22 of the GDPR and § 31 of the BDSG. In the jurisprudential discussion, more and more voices are in favour of regulating algorithms.[89] Regulation can start with the codes as well as with the use of AI.

So far, the source code is not public and is therefore not open to examination. The parameters used, their weighting and possible correlations remain hidden from the public. Sometimes, there is talk of a "black box algorithm".[90] This can be countered with transparency and traceability of algorithm-based decisions.

However, there should not be just one European law that regulates all algorithms and AI in all areas of application. Rather, each area should provide for individual regulations.[91] In fact, creating transparency appears to be the most difficult task, as neither data protection officers in companies nor the data protection authorities of the German federal states have the necessary

[87] C Feldhusen, 'Kreditwürdigkeitsprüfung: Wieviel Würdigung erlaubt die Prüfung nach Erlass der Immobiliar-Kreditwürdigkeitsprüfleitlinien-Verordnung?' [2019] WM , 97, 100.
[88] A Caliskan/JJ Bryson/A Narayanan, Semantics derived automatically from language corpora contain human-like biases, arXiv:1608.07187v4 [cs.AI], Cornell University, 2016, p. 1 ff.
[89] B Zypries, 'Digitalisierung erfordert Regulierung und Deregulierung' [2019] ZRP, 33; J Gerberding/GG Wagner, 'Qualitätssicherung für "Predictive Analytics" durch digitale Algorithmen' [2019] ZRP, 116; Martini, 'Algorithmen als Herausforderung für die Rechtsordnung' (n 36) 1017, 1020 f.
[90] Martini, 'Algorithmen als Herausforderung für die Rechtsordnung' (n 36) 1017, 1018; F Pasquale, *The Black Box Society* (Harvard University Press 2015) passim.
[91] So also Gerberding/Wagner, 'Qualitätssicherung für "Predictive Analytics" durch digitale Algorithmen' (n 90) 116.

knowledge or capacities to review millions of algorithms and AI.[92]

Further proposals for regulation can be found in Martini's work, e.g. a duty to justify algorithms and their decision or an independent review body.[93] A broad-based regulatory approach is to be endorsed.

Conclusions.

Already today, the use of algorithms is steadily increasing and it is foreseeable that AI will dominate more and more areas of life in the future. As has been shown, algorithms harbor the danger of discrimination and give reason for regulation. This is mainly due to the immanent lack of transparency. When considering and regulating algorithm-based AI, a clear distinction should be made between it and rule-based software. With regard to the latest proposal for an AI regulation of the European Commission, the broad definition of AI is subject for criticism.

In the USA, protection against discrimination by algorithms and AI follows in particular from the 14th Amendment and the Civil Rights Act. This covers various forms of discrimination. Affirmative actions are permissible, provided that certain conditions are met, in particular purpose and means.

In Germany, constitutional protection against discrimination is based on Article 3 of the German Constitution. The use of predictive policing with reference to personal data faces high constitutional hurdles. In the general civil law context, however, Art. 3 GG is only applicable under very strict conditions, as it otherwise has no third-party effect.

The AGG covers numerous prohibited forms of discrimination and grants comprehensive protection. Only the previous understanding of treatment in the sense of § 3 para. 1 AGG with the requirement of human action or omission leads to the fact that actions of algorithms are not covered.

Particularly in labour law, banking and capital market law, as well as insurance and tenancy law, attention must be paid to standards of the GG, the GDPR, the BDSG and the AGG when using algorithms and AI.

In order to prevent discrimination by software from increasing, the regulation of algorithms should be strengthened. Numerous, cumulative regulatory approaches are available for this purpose. In order to prevent discrimination, a regulation is necessary that obliges transparency in the making of a decision.

[92] But so Zypries, 'Digitalisierung erfordert Regulierung und Deregulierung' (n 90) 33.
[93] Martini, 'Algorithmen als Herausforderung für die Rechtsordnung' (n 36) 1017, 1020 f.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Post-quantum encryption and privacy regulation: Can the law keep pace with technology?

LUIGI BRUNO
Doctor of Civil Law (D.C.L.) candidate at McGill University, Faculty of Law
ISABELLA SPANO
Doctor of Civil Law (D.C.L.) candidate at McGill University, Faculty of Law

Abstract

Using an interdisciplinary law and computer science approach, this article argues that quantum computing must push lawmakers to implement more dynamic privacy regulation to cushion quantum computing's impact on data protection and privacy.

This article highlights the EU GDPR position as the global standard for data protection and privacy regulation. The GDPR has ignited a legal standardization phenomenon, whereby many jurisdictions are shaping their privacy regulation based on the GDPR. A move by EU lawmakers to amend the GDPR to embed post-quantum encryption requirements dynamically would ignite a global paradigm shift. This would result in forward-looking protection of data subjects' rights that extends beyond quantum computing perils. It would also signal that lawmakers' intention to making privacy regulation dynamic, thus enabling it to cope with future threats by being ahead of the technological disruption curve.

Keywords: Privacy Law; GDPR; Quantum Computing; Encryption; Data Protection Law; Technology Law.

Introduction.

Quantum computing is still far from mainstream adoption and is currently only used for scientific research purposes. Nevertheless, its impact on existing encryption algorithms and data protection and privacy regulation is already generating threats that require attention and consideration.

This novel computing paradigm came under the spotlight in 2019 when Google's AI Quantum team announced that it had achieved quantum supremacy.[1] Google announced the achievement via an article in Nature, which sparked controversy with IBM.[2] In the article, Google's team argued that their quantum processor (a 54 qubits "Sycamore") had taken about 200 seconds to perform a task that would have taken a state-of-the-art classical supercomputer approximately 10'000 years to complete. [3] A classical supercomputer is one of today's fastest high-performance systems.[4] Google's significant improvement in computational speed represents an experimental achievement of quantum supremacy, at least for the particular task tested.[5]

One year later, China's government announced that a team of its scientists had also achieved quantum supremacy. China made its announcement in an article in Science, wherein PRC's scientists declared that their achievement resulted from a quantum computer based on a different technology than Google's.[6]

These announcements are symptomatic of an ongoing race to quantum supremacy among superpowers - a race fuelled by quantum computing's promises to disrupt and improve research in chemistry, [7] biology, space exploration, artificial intelligence, and more.

Nevertheless, disruption also has side effects. Extensive research has shown that quantum computing can break modern symmetric and asymmetric

[1] Frank Arute et al., 'Quantum supremacy using a programmable superconducting processor' (2019) Nature 574, 505.
[2] Edwin Pednault et al., 'On "Quantum Supremacy"' *IBM* (21 October 2019) <https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/5>.
[3] Arute et al., 'Quantum supremacy using a programmable superconducting processor' (n 1).
[4] William L. Hosch, 'Supercomputer' *Encyclopedia Britannica* (2019) <https://www.britannica.com/technology/supercomputer> accessed 20 November 2019.
[5] *Ibid.*
[6] Han-Sen Zhong et al., 'Quantum computational advantage using photons' (2020) Science 370, 1460.
[7] Bryan Walsh, 'Why quantum computing matters' Axios (26 August 2020) <https://www.axios.com/quantum-computing-google-ibm-b0b90670-a36b-443a-b45f-eff3ceb79ec2.html> accessed 8 January 2020.

cryptography, [8] threatening current data protection and privacy practices. Regulation and laws worldwide rely on encryption as a tool to protect personal information online. The pace of development in quantum computing should inspire legislators and supervisory authorities alike to swiftly reconsider how laws and regulation can cushion quantum's impact on data protection.

This article discusses the impact of quantum computing on modern cryptographic algorithms from the interdisciplinary perspective of law and computer science. Its goal is to explore how data protection and privacy regulation need to be reimagined to keep up with technological development.

The remainder of this article is divided into four parts. The first part introduces quantum computing by showing how it differs from classical computing. The second part discusses quantum computing's impact on current encryption practices and, consequently, data protection and privacy. The third part argues that quantum computing's threats to encryption are a cautionary tale for data protection and privacy bodies, regulators and legislators, who face the challenge of technology exponentially outpacing regulation. The fourth and last part explores existing post-quantum cryptography initiatives and the future of data protection and privacy regulation.

1. Quantum computers versus classical computers: A tale of two worlds.

Quantum computers leverage quantum mechanics' laws to use quantum bits, in short *qubits*, as the basic data unit. These laws generate phenomena that enable qubits to be in multiple states of *|0⟩* and *|1⟩* simultaneously and correlate their measurement and states.[9] Qubits' very nature brings forward a new paradigm that does not map onto classical concepts. Essentially, qubits are in a linear combination of a 0 state and a 1 state, which is neither "AND" nor "OR." Therefore, through this paradigm, quantum computers perform operations so that the probabilities of reaching the right results are enhanced, while the probabilities of getting the wrong results are depressed.[10]

On the other hand, classical computers differ from quantum computers because they do not leverage quantum mechanics' properties and advantages to perform computation.[11] A classical computer—that is, one that can be modelled by a deterministic Turing machine—uses *bits* as the basic data unit. Users input instructions that are converted in binary code of 0s and 1s and are then translated into electrical signals to operate the transistors that compose the Central Processing Unit. 0 indicates "OFF," and 1 "ON." According to this logic, classical computers can only perform operations for determined values of 0 and 1.

2. The relevance of quantum computing for encryption.

[8] Vasileios Mavroeidis et al., 'The Impact of Quantum Computing on Present Cryptography' (2018) International Journal of Advanced Computer Science and Applications 9, 405.
[9] Vasileios Mavroeidis et al., 'The Impact of Quantum Computing on Present Cryptography' (n 8).
[10] National Academy of Engineering, *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2018 Symposium* (National Academies Press 2019).
[11] Jack Hidary, *Quantum Computing: An Applied Approach* (Springer 2019).

In 1982 Richard Feynman brought the idea of quantum computing to light.[12] However, the scientific community's interest in quantum computing increased sharply in 1994 when the mathematician Peter Shor developed the famous eponymous algorithm.

Shor's algorithm allows quantum computers to "*find the prime factors of large numbers efficiently*," [13] that is, "*with an exponential speed-up when compared to the best-known classical algorithm.*"[14] The problem of finding the prime factors of large numbers is the foundation of most of today's secure online communication.

The factorization problem at the heart of Shor's algorithm is vital to secure most of today's online communication. In this light, Gamble argues that the efficiency of Shor's algorithm should be seen:

[…] in a time of practical relevance, which is beyond the capability of state-of-the-art classical algorithms. […] The security of nearly every online transaction today relies on an RSA cryptosystem that hinges on the intractability of the factoring problem to classical algorithms.[15]

The RSA cryptosystem is a building block of the current internet infrastructure used to secure most online communication.[16] Its importance cannot be overstated since over 69%[17] of all websites communicate relying on the secure version of the HTTP protocol (the so-called HTTP Secure protocol), which is based on RSA encryption.[18]

The RSA algorithm's one-way function is the same integer factorization problem at the heart of Shor's algorithm. By recalling high school mathematics notions, it is easy to see that multiplying two large prime numbers is simple. However, the operation of factoring the resulting product is incredibly difficult.[19] Most of the commonly used forms of RSA encryption are currently based on the 2048 bits number factorization. Factoring any number larger than that is considered to be almost impossible for a classical computer.[20]

According to the MIT Technology Review, a team of scientists at Google and at the KTH Royal Institute of Technology has shown that a 20-million qubits quantum computer could factor 2048 RSA integers and thus break encryption in only eight hours.[21] However, a 20-million qubits processor seems a distant

---

[12] Richard P. Feynman, 'Simulating Physics with Computers' (1982) International Journal of Theoretical Physics 21, 467.
[13] Franklin de Lima Marquezino et al., 'Shor's Algorithm for Integer Factorization' in Franklin de Lima Marquezino et al. (eds), *A Primer on Quantum Computing* (Springer 2019).
[14] *Ibid.*
[15] National Academy of Engineering, *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2018 Symposium* (n 10).
[16] Christof Paar and Jan Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners* (Springer 2009).
[17] W3 Techs, 'Web Technology Surveys' <https://w3techs.com/technologies/details/ce-httpsdefault> accessed 20 January 2021.
[18] For further information on the Hyper-Text-Transfer-Protocol Secure (HTTPS) see James F Kurose and Keith W Ross, *Computer Networking: A Top-Down Approach* (Pearson 2013).
[19] Christof Paar and Jan Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners* (n 16).
[20] Emerging Technology from the arXiv, 'How a quantum computer could break 2048-bit RSA encryption in 8 hours' *MIT Technology Review* (30 May 2019) <https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/>.
[21] *Ibid.*

reality compared to the 54 qubits processor that Google used to declare quantum supremacy in 2019.

At the current pace of innovation, a 20-million qubits processor could take 25 years or more to be produced.[22] Or it could take less, much less. History is filled with failed attempts to predict the rate of innovation.[23]

This impossibility to accurately forecast when quantum computing will be capable of quickly breaking existing encryption methods prospect raises technical and regulatory questions *vis-à-vis* its critical implications for data protection and privacy. For instance, information intended to be stored for extended periods, in domains such as banking, defence, and foreign policy, should be secured with cryptographic algorithms that are quantum-proof as soon as possible. Encrypted packets of personal and sensitive information could be captured online today and be decrypted in the future, once quantum computers have become widely available and powerful enough. Although decrypting a credit card number three decades from now would probably prove unfruitful for the attackers, the same cannot be said for social security numbers and other personally identifiable information.

Therefore, quantum computers' ability to efficiently solve complex factorization problems poses a threat to current cryptographic systems and, consequently, to the data protection and privacy capabilities they offer. Mathematicians aware of these threats have launched initiatives aiming at keeping data and privacy protected in a post-quantum world. These initiatives have given rise to post-quantum encryption algorithms that leverage mathematical operations that cannot be efficiently solved using quantum computation. Many of these algorithms are freely available online.

The US National Institute of Standards and Technology (NIST) has been the first public body to acknowledge the threat that quantum computing poses to encryption. In 2017, the NIST launched a Post-Quantum Encryption Standardization project and invited mathematicians and cryptography experts to submit proposals for encryption algorithms that could withstand attacks carried using quantum computation.[24]

However, there is no doubt that standardization does not equal regulation. Data protection and privacy laws that hinge on encryption as a technical measure to prevent breaches ought to be reimagined in the face of quantum computing. NIST's standardization effort will only prove marginally successful in maintaining the security of today's internet communication unless its outcomes are swiftly absorbed by regulation and enforced by data protection authorities.

3. A privacy and data protection regulatory challenge: slow regulation for fast tech.

[22] Emerging Technology from the arXiv, 'How a quantum computer could break 2048-bit RSA encryption in 8 hours' (n 20).
[23] For a timeline of failed technology predictions see Visual Capitalist <https://www.visualcapitalist.com/a-timeline-of-failed-tech-predictions/> accessed 10 Jan 2021.
[24] NIST, 'NIST Asks Public to Help Future-Proof Electronic Information' (20 December 2016) <https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information> accessed 11 January 2021.

NIST's standardization initiative is a warning for governments and privacy and data protection bodies alike that legislative and regulatory action is needed. For instance, European lawmakers and data protection authorities are aware that personal information must be protected from quantum computing perils.[25] However, the breadth of the measures required to ensure continued and consistent protection while quantum computers are developed, become available, and are eventually adopted may not have been fully grasped yet.

This legislative inertia might rest on the assumption that it will take quantum computing a generation or more before it becomes a critical problem for data protection and privacy.[26] This assumption might be severely flawed, considered that technology forecasting rarely yields satisfying results, mainly when global superpowers are competing to be the fastest to develop the best quantum technology.[27] Therefore, it would not be surprising if quantum computing development accelerated several orders of magnitude over the next few years.

Legislators ought to consider this possibility since one of the most significant challenges that they continue facing in creating and implementing regulatory frameworks is the different pace at which technology and the law move. By its nature, the law is static and developed to respond to societal changes *a posteriori*. Norms require time to be implemented within a system, whereas technology is swift and thrives dynamically, in continuous evolution.

For instance, the European Union General Data Protection Regulation (GDPR)[28] was adopted in 2018 to replace the 1995 Data Protection Directive.[29] The latter was developed and introduced at the dawn of the internet era when all but a handful of visionaries saw the World Wide Web's potential and perils. Many technologies evolved exponentially during the six years that elapsed from the moment the European Commission proposed a reform to the 1995 Directive to adopting the GDPR. One of these technologies is Machine Learning, which, until the advent of the GDPR, was used to process personal

[25] The European Data Protection Supervisor has recognized the relevance of NIST's standardization process and stressed that the uncertainty of quantum computing development will require solutions to protect data. See Lukas Olejnik and Robert Riemann, 'TechDispatch #2/2020: Quantum Computing and Cryptography', *Eur. Data Prot. Supervisor* (7 August 2020) <https://data.europa.eu/doi/10.2804/603798> accessed 14 January 2020. In the United States, Dr. Jill Pipher of Brown University presented "No Longer Secure: Cryptography in the Quantum Era" at a Capitol Hill lunch briefing, in December 2019. In the briefing, Pipher also discussed the consequences of quantum computing on cybersecurity. See Cynthia Brumfield, 'The Race for Quantum-Proof Cryptography' *CSO* (10 December 2019) <https://www.csoonline.com/article/3488857/the-race-for-quantum-proof-cryptography.html> accessed 15 December 2020.

[26] See Olejnik and Riemann ("Based on what we know today there is no immediate threat posed by a quantum computer in the foreseeable future.").

[27] Not surprisingly, quantum computing development has been compared to the so-called "space race", with numerous superpowers investing and competing to achieve quantum supremacy. See Walter G. Johnson, 'Governance Tools for the Second Quantum Revolution' (2019) Jurimetrics 59, 490–491.

[28] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[29] 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 [1995] OJ L281/31.

data almost without any regulatory constraints.[30]

The natural consequence of the dynamic between law and technology is that legislative and regulatory bodies' attempts to keep technology within their grasp often fail or result unsatisfactory.[31] This outcome can be due to the inability to translate the fast-paced dynamism of technology into the law's static language. When it comes to data protection and privacy, the price for excessively static, and often late, regulation is paid directly by data subjects, whose privacy is threatened by normative gaps. Hence, to maintain adequate normative protection of privacy rights *vis-à-vis* technological innovation and disruption, a proactive, dynamic and forethinking legislative approach is required.

Such an approach can be partly identified in one of the core principles of the GDPR: Privacy by Design. The principle provides that systems processing personal data should be designed to ensure privacy protection.[32] In other words, Privacy by Design aims to integrate proactive privacy safeguards in the design phase of systems that process personal data. The idea of Privacy by Design requires dynamism of privacy safeguards' implementation, with organizations preventing risks rather than patching up damages from materialized data breaches.

In 2010, the International Conference of Data Protection and Privacy Commissioners stated that "Privacy by Design [is] an essential component of fundamental privacy protection" and encouraged lawmakers to include this principle in future privacy and data protection regulatory frameworks.[33] Privacy by Design, as embraced by Article 25 of the GDPR, represents the recognition by the EU of its foundational importance in data protection efforts.[34] This leads to questioning whether the GDPR as a whole proposes a dynamic approach that can respond to privacy risk and threats stemming from future technological innovations such as quantum computing. This question's relevance cannot be overstated, given that the GDPR has *de facto* ignited a process of global legal harmonization.[35] For instance, other jurisdictions, such as California[36] and Quebec[37], have adopted or are in the process of adopting laws that are primarily inspired by the GDPR.

---

[30] For an overview of the history of data protection and privacy regulation see European Data Protection Supervisor <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed on 11 January 2021).

[31] Mark Fenwick et al., 'Regulation Tomorrow: Strategies for Regulating New Technologies' in Toshiyuki Kono et al. (eds), *Transnational Commercial and Consumer Law* (Springer 2018) 153-155.

[32] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, para 25.

[33] Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners (27-29 October 2010) <https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf> accessed 16 January 2021.

[34] Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) Oslo Law Review 4, 107.

[35] On the effects of the GDPR on global data protection see Tiffany Curtiss, 'Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies' (2016) Washington Journal of Law, Technology and the Arts 12, 95; Christopher Kuner et al., 'The GDPR as a Chance to Break Down Borders' (2017) 7 International Data Privacy Law 7, 231; Dulce Lopes, 'GDPR - Main International Implications' (2020) European Journal of Privacy Law and Technology 9.

[36] California Consumer Privacy Act of 2018 (USA).

[37] Quebec Bill N.64 (CA).

Analysing the difference between the concept of Privacy by Design originally theorized by privacy scholar Ann Cavoukian and the novel iteration of the same principle within the GDPR may help answering this question. Theoretically, Privacy by Design requires a dynamic and continuously evolving approach to data protection, mirroring the dynamism of technological development. Privacy by Design aims to consistently protect personal data regardless of how and in which direction technology evolves. According to Cavoukian, "*[p]rivacy must become integral to organizational priorities, project objectives, design processes, and planning operations*."[38]

Cavoukian's theorization of Privacy by Design proposes a multidimensional approach to privacy protection for organizations. Vertically, this approach requires organizations to embed privacy in their systems and technologies by default, through privacy engineering.[39] Horizontally, it requires organizations to reimagine their business under the overarching theme of privacy. Overall, Cavoukian's approach aims to ensure that organizations anticipate and prevent privacy-invasive events before they happen.[40]

The current approach to Privacy by Design proposed by Article 25 of the GDPR greatly emphasizes the principle's vertical dimension rather than its multidimensionality. However, the horizontal dimension would ensure threats like the one posed by quantum computing to be anticipated and dealt with swiftly, without requiring additional legislation or continuous reforms.

The limitation of the reach of the principle of Privacy by Design in the GDPR seems based on risk analysis. The more dynamic a law, the more it will inevitably encounter feasibility and continuous compliance issues. Hence, the EU lawmakers faced the risk of creating an unenforceable soft law instrument had it excessively and unclearly generalized the norm's content. On the other hand, the opposite would have led to an impossibly demanding framework that would have unfairly disadvantaged small businesses over Big Tech companies, with the latter having the resources to ensure compliance.[41]

It is necessary for the GDPR and, by extension, GDPR-inspired regulation worldwide to provide a more encompassing and dynamic privacy governance framework. One that would require little to no amendments to the regulation, to ensure that forthcoming privacy risks and threats such as quantum computing are minimized seamlessly and consistently over time. Dynamic privacy and data protection regulation should favour proactive wording to push organizations to stay ahead of the disruption curve. In the case of quantum computing, this means requiring organizations to implement the forthcoming NIST post-quantum encryption standards without waiting for the adoption of additional legislation.

---

[38] Ann Cavoukian, 'Privacy by Design: the 7 Foundational Principles' *Privacy Security Academy* (August 2020) <https://www.privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf> accessed 8 December 2020.

[39] Sean Brooks et al., 'An Introduction to Privacy Engineering and Risk Management' *NIST* (7 January 2017) <https://doi.org/10.6028/NIST.IR.8062> accessed 11 December 2020.

[40] Ann Cavoukian, 'Privacy by Design: the 7 Foundational Principles' (n 38).

[41] Even in the GDPR's current form, the EU has registered hardships in GDPR compliance for small businesses. On the matter see the '2019 GDPR Small Business Survey', GDPR.eu (May 2019) <https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf> accessed 14 January 2021.

4. Conclusions: Post-quantum cryptography and the future of data protection regulation.

Quantum computing must start the conversation on the implementation of more dynamic privacy and data protection regulation. NIST's effort to reach a standardized set of post-quantum encryption algorithms should inspire legislators and privacy authorities worldwide to start the necessary process of reforming existing and introducing new regulatory frameworks.

NIST has explicitly warned organizations about the threats that quantum computing presents already today to encrypted data and what risks this entails for data subjects. NIST's recommendation is unequivocal: prepare today for the privacy breach of tomorrow. Lawmakers should embrace this proactive and forward-thinking approach and embed it in data protection and privacy regulation. Without it, it will be difficult to achieve regulatory dynamism and cope with forthcoming technological changes that may affect data protection and privacy.

NIST's Post-Quantum Cryptography Standardization project aims to standardize a set of the most effective quantum-resistant cryptographic algorithms. Its goal is to solicit, evaluate and select quantum-resistant public-key cryptographic algorithms devised by mathematicians and cryptography experts worldwide.[42] Public-key algorithms, such as RSA, underpin today's infrastructure that allows us to communicate online securely. Therefore, NIST has chosen to limit its standardization efforts only to these algorithms, at least for the time being.

NIST has announced the beginning of its third selection round on July 22, 2020.[43] The expectation is that by the end of this phase, NIST will shortlist one or two quantum-resistant encryption algorithms that will ultimately compose its standard. The current deadline for the publication of the first official standard is 2022, even when considering potential pandemic-related slowdowns. At the same time, NIST will provide organizations with technical guidance on implementing the standardized algorithms.

In the meantime, to ease the transition, NIST has recently published a whitepaper in which it first paints the picture of the impact of quantum computing on existing – or classical – encryption. It then brings forward the challenges linked with implementing post-quantum encryption once the standardization process will have been concluded.[44]

Lawmakers and privacy authorities outside of the US should closely monitor NIST's standardization project's outcome, [45] as the EU Agency for Cybersecurity

---

[42] NIST, 'Post-Quantum Cryptography' *NIST* (6 January 2017) <https://csrc.nist.gov/projects/post-quantum-cryptography> accessed 19 January 2021.

[43] NIST, 'NIST's Post-Quantum Cryptography Program Enters "Selection Round"' *NIST* (22 July 2020) <https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round> accessed 4 January 2021.

[44] NIST, 'Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms' NIST (28 April 2021) <https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final> accessed 28 June 2021.

[45] NIST's efforts have already been recognized by agencies such as the French *Agence National de la Sécurité des Systèmes d'Information* (ANSSI), which published a paper on Quantum Key Distribution. In its paper, ANSSI

(ENISA) is already doing. The GDPR has de facto become the global gold standard for data protection and privacy regulation. An increasing number of jurisdictions are shaping their privacy regulation based on the GDPR, mainly to ensure adequate data protection to transfer data from and to the EU. Providing free and secure data transfer with the EU is a priority for states and organizations alike, given the single EU market's economic relevance. [46] Therefore, a potential move by Brussels' lawmakers to prescribe the implementation of NIST's post-quantum encryption standard, at least to those organizations potentially impacted by the technology, would ignite a paradigm shift. It would not only project international data protection into its post-quantum future, but it would also signal that data protection and privacy regulation are most effective when they look at the future of technology. In such a case, foreign jurisdiction would inevitably follow the EU's lead, thus setting up a new global standard for privacy protection while renewing the conversation on how regulation ought to be designed and implemented.

Doing so would not require much regulatory effort from the EU. For what concerns explicitly encryption, the GDPR indicates in its article 32 the obligation for organizations to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk".[47] In this light, ENISA has recently released a study examining the current state of the standardization process of post-quantum encryption, including describing the finalist algorithms chosen by NIST. [48] The study has a forward-looking approach, taking into consideration the time that will be required for NIST to complete its standardization process. It also offers organizations two proposals for implementing immediate solutions that could already protect the confidentiality of their data against quantum-enabled attacks.[49] Hence, the European Data Protection Board (EDPB) could release additional guidelines clarifying quantum computing's impact on encryption a legal perspective and requiring organizations to follow ENISA's proposals and then implement NIST's standard to ensure compliance with the GDPR.

On the one hand, this would result in a stronger, more encompassing, and forward-looking protection of data subjects' privacy rights. On the other hand, it would signal that lawmakers and supervisory authorities are keen to make privacy regulation dynamic. A dynamic regulatory framework would ultimately be capable of coping with forthcoming threats by relying on additional sources, such as standards and soft-law instruments, without needing constant amendments or reforms.

---

advises caution in the application of NIST's algorithms, and suggests "combin[ing] them with current mechanisms in order to avoid any security regression linked to immature designs." ANSSI, 'Should Quantum Key Distribution Be Used for Secure Communications' *ANSSI* (4 May 2020) <https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/> accessed 16 January 2021.

[46] Dulce Lopes, 'GDPR - Main International Implications' (2020) European Journal of Privacy Law and Technology 9, 14.

[47] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, para 32.

[48] ENISA, 'Post-Quantum Cryptography: Current state and quantum mitigation' ENISA (3 May 2021) <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation> accessed 24 June 2021.

[49] *Ibid.*

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Cookies e consenso: le nuove prospettive.

Cookies and consent: the new perspectives.

MARIA ROBERTA PERUGINI
IUSINTECH co-founder, Lawyer

Abstract

Fin dagli esordi della disciplina del marketing comportamentale sono stati evidenziati gli effetti potenzialmente deleteri (in termini di alto rischio di violazioni dei dati personali e dei diritti degli utenti) derivanti dell'uso di identificativi univoci online, tanto più in quanto usati in sinergia con i più sofisticati strumenti di data mining.

L'articolo schematizza la storia e le problematiche collegate all'uso di marcatori online per farne emergere con chiarezza e concretezza il punto di arrivo sulle azioni oggi richieste per operare legittimamente i trattamenti a fini di marketing e profilazione che si basano sull'uso di queste tecnologie. Infine, l'articolo affronta brevemente le nuove frontiere del behavioural advertising nel contesto a tendere "cookieless".

Since the very beginning of the discipline of behavioural marketing, the potentially detrimental effects (in terms of high risk of personal data violations and users' rights) deriving from the use of online unique identifiers have been highlighted, even more so as they are used in synergy with the most sophisticated data mining tools.

The article schematizes the history and the problems related to the use of online identifiers in order to highlight with clarity and concreteness the actions required at present to legitimately operate the treatments for marketing and profiling purposes which are based on the use of these technologies. Finally, the article briefly addresses the new frontiers of behavioural advertising in the 'cookieless' context.

Parole chiave: Cookies; GDPR; Direttiva e-Privacy; Proposta di Regolamento e-Privacy; Pubblicità comportamentale; Pubblicità programmatica; Monitoraggio online; Profilazione; Consenso; senza Cookies; EDPB; Corte di Giustizia.

Keywords: Cookies; GDPR; E-Privacy Directive; Proposal for an e-Privacy Regulation; Behavioural advertising; Programmatic advertising; Tracking online; Profiling; Consent; Cookieless; EDPB; Justice Court.

Introduzione.

Parlare di cookies (e altri marcatori della navigazione web) significa parlare di behavioural advertising.

Fin dagli esordi della disciplina del marketing comportamentale sono stati evidenziati gli effetti potenzialmente deleteri (in termini di valutazione di alto rischio di violazioni dei dati personali e dei diritti degli utenti) derivanti dell'uso di identificativi univoci online, tanto più in quanto usati in sinergia con i più sofisticati strumenti di data mining.

Ciò che accade è che si sono affermate tecniche di "targetizzazione" delle inserzioni pubblicitarie via via sempre più precise, che cercano di indirizzare i contenuti agli utenti mediante la conoscenza sempre più esatta delle loro propensioni ed esigenze.

Il marketing comportamentale funziona sfruttando le tecnologie di tracciabilità (tracking) delle operazioni dei navigatori online: attraverso l'analisi di marcatori, soprattutto cookies di prima e di terza parte [1], è possibile risalire al numero di visite a determinati siti, alle ricerche effettuate sul web, agli acquisti conclusi su certi e-shop, al tempo globale passato su internet, ma anche all'attività sui social ...

Tutti questi dati vengono utilizzati per tracciare un profilo "pubblicitario"

[1] I cookie di "prima parte" sono quelli rilasciati nel terminale dell'utente direttamente dall'editore/gestore del sito che l'utente sta visitando; quelli di "terza parte" sono invece creati da dominî differenti da quello in cui si sta navigando, generalmente grandi piattaforme di advertising (la principale è Double Click di Google): i cookies permangono nel terminale dell'utente e tracciano la sua navigazione segnalando ai server dell'emittente le attività che l'utente svolge online. In questo modo, specialmente i cookie di terza parte diventano strumento essenziale, ed estremamente efficiente, per una profilazione dell'utente cross-site, che produce profili altamente dettagliati e precisi del consumatore e di conseguenza permette da un lato la personalizzazione del messaggio promozionale e dall'altro il suo inserimento in target group altamente definiti, da utilizzare nelle campagne di retargeting nell'ambito del programmatic advertising.

personalizzato di ogni singolo navigatore, il quale viene inserito in appositi filtri e dunque viene raggiunto da advert appositamente pensati per le sue caratteristiche. Dunque, è probabile che se, ad esempio, un utente ha acquistato un libro su Amazon, altre pubblicità su siti diversi gli proporranno libri simili o dello stesso autore.

Lo scopo di tale strategia comunicativa è quella di "contattare" o "ricontattare" gli utenti sulla base delle loro precedenti azioni su internet, al fine di portare quel determinato utente a concludere l'azione commerciale sperata (una cosiddetta "conversione": vale a dire, effettuare un acquisto o completare un acquisto "abbandonato", lasciare i propri contatti, iscriversi alla newsletter, etc).

Figura 1

In particolare, si parla di remarketing o retargeting per indicare, nell'accezione più ampia dei termini, quella forma di marketing comportamentale basata sull'utilizzo dei cookies consistente nell'invio di messaggi/annunci pubblicitari agli utenti che sono transitati su uno specifico sito affinché ritornino sullo stesso sito per effettuare/completare un'azione significativa.

Più specificamente, il retargeting è lo strumento che permette di recuperare la comunicazione con l'utente (non convertito), mostrandogli annunci o inserzioni pertinenti mentre naviga sul web, mentre il remarketing (che si rivolge ai contatti, che hanno già eseguito la conversione e di cui si possiedono nome, cognome e/o altre informazioni di contatto) "riaggancia" l'utente tramite l'invio di messaggi diretti allo stesso (email) altamente "targettizzati" (con una proposta precisa e personalizzata) al fine di tentare di coinvolgerlo ancora una volta e convincerlo a trasformare le proprie intenzioni in azioni concrete.

Figura 2[2]

Ovviamente gli "over the top" (comunemente richiamati come OTT), come Google e Facebook, hanno elaborato propri strumenti di tecnologia pubblicitaria per attivare campagne di marketing comportamentale che mettono a disposizione di editori e inserzionisti: ad esempio Google AdWords o Facebook Ads, attraverso i quali gli inserzionisti possono pubblicare rispettivamente nelle pagine di ricerca di Google o all'interno di Facebook i loro annunci (di testo, banner, video) che verranno mostrati a persone potenzialmente interessate.

Enterprises' internet presence (use of internet ads by type, websites, social media), 2018

	Internet advertising	Contextual advertising	Behavioural targeting	Geo-targeting	Other method of targeted advertising	Having a website	Using social media*
	% of enterprises	% of enterprises using internet ads				% of enterprises	
EU-28	26	80	32	37	38	77	47
Belgium	30	71	33	38	43	84	58
Bulgaria	21	78	23	28	33	51	34
Czechia	31	89	32	36	41	93	36
Denmark	47	71	33	44	41	96	68
Germany	27	86	26	32	31	87	45
Estonia	28	74	54	40	58	78	40
Ireland	34	75	38	51	45	79	68
Greece	28	81	38	44	50	65	50
Spain	25	72	40	35	50	76	51
France	19	87	33	32	41	69	41
Croatia	27	68	30	22	24	73	45
Italy	21	75	25	38	42	71	44
Cyprus	33	83	48	55	9	71	67
Latvia	26	76	11	19	24	63	30
Lithuania	35	79	37	26	44	78	50
Luxembourg	36	63	25	33	35	83	54
Hungary	21	79	28	33	37	66	38
Malta	47	73	42	46	69	82	73
Netherlands	34	89	43	45	49	94	68
Austria	32	73	30	38	30	88	53
Poland	26	88	30	27	36	67	27
Portugal	16	75	42	45	55	63	46
Romania	15	90	41	32	38	44	35
Slovenia	22	93	30	31	5	84	47
Slovakia	25	75	32	23	42	76	39
Finland	37	83	49	44	31	96	63
Sweden	44	60	23	31	26	92	65
United Kingdom	32	78	37	47	40	82	63
Iceland	50	:	:	:	:	81	79
Norway	45	63	26	42	42	78	72
Montenegro	:	62	31	37	66	:	50
North Macedonia	:	:	:	:	:	:	:
Serbia	31	65	36	44	36	82	39
Turkey	15	82	53	63	32	66	46
Bosnia and Herzegovina	22	58	30	35	35	65	:

* Data on social media refer to 2017
(:) data not available
Source: Eurostat (online data codes: isoc_cismt, isoc_ciweb)

eurostat

Figura 3

È importante rilevare che questo mercato vede un fortissimo sviluppo anche

[2] Immagine estratta dal seguente sito: https://www.criteo.com/it/wp-content/uploads/sites/9/2017/07/Criteo-Retargeting101-eBook-IT.pdf

grazie all'affermazione della navigazione e-commerce tramite le app piuttosto che tramite il tradizionale sito web: uno dei maggiori operatori mondiali nel retargeting, Criteo, ha stimato che già nel 2018 le vendite In-App rappresentavano fino al 65% delle transazioni online in Europa e che le app fanno registrare anche tassi di "conversione" (ossia di vendita) tre volte superiori rispetto a quelli del mobile web.

Figura 4[3]

Quindi Criteo ha sviluppato un sistema App Retargeting, che raggruppa le app di numerosi editori e consente di seguire l'utente nei suoi passaggi da un'app all'altra (ad esempio, da un'app di prenotazione viaggi ad una di gioco) in modo da tenerlo "agganciato" e ricondurlo con facilità alla transazione abbandonata.

Criteo ha dichiarato che tramite il proprio sistema "Criteo App Advertising" è in grado di acquisire dati da 1,2 miliardi di consumatori ogni mese, di avere una visione a 360 gradi e in tempo reale del comportamento di navigazione di un consumatore su dispositivi, browser e 550.000 app che il sistema utilizza per attirare ciascun utente con annunci ottimizzati in tempo reale in base all'intenzione di acquisto individuale e al contesto di navigazione, riportandolo all'app dove ha iniziato l'acquisto per completarlo.

Figura 5

Criteo afferma altresì di essere il grado di identificare in modo univoco e

[3] Immagine estratta da: https://www.criteo.com/it/wp-content/uploads/sites/9/2018/09/18_GCR_Q2_Report_EMEA_IT.pdf

anonimo su più di 2 dispositivi gli utenti da cui proviene oltre il 40% di tutte le vendite online.

Questo tipo di approccio comunicativo comporta naturalmente l'immagazzinamento di un numero molto elevato di informazioni sugli utenti del web.

Nel 2019 Apple ha introdotto sull'App store l'obbligo per gli sviluppatori di adottare "etichette" che indicano quali categorie di dati personali vengono raccolti dalle apps. Le categorie sono 14, tra cui la cronologia della navigazione, le ricerche fatte, gli acquisti, la geolocalizzazione, le informazioni di contatto, i dati finanziari…
Il fornitore di servizi IT pCloud ha usato questa classificazione per censire il livello di dati raccolti per scopi commerciali da una serie di app tra le più popolari nel mondo.

Come mostrano le immagini, Facebook e Instagram sono quelle che usano più dati degli utenti (12 categorie su 14) per l'internal marketing (l'86%!), mentre sempre Instagram si distingue per la più massiva condivisione delle informazioni personali degli utenti con terze parti, sempre a fini di marketing, raccogliendo il 79% dei dati di 11 delle 14 categorie elencate.

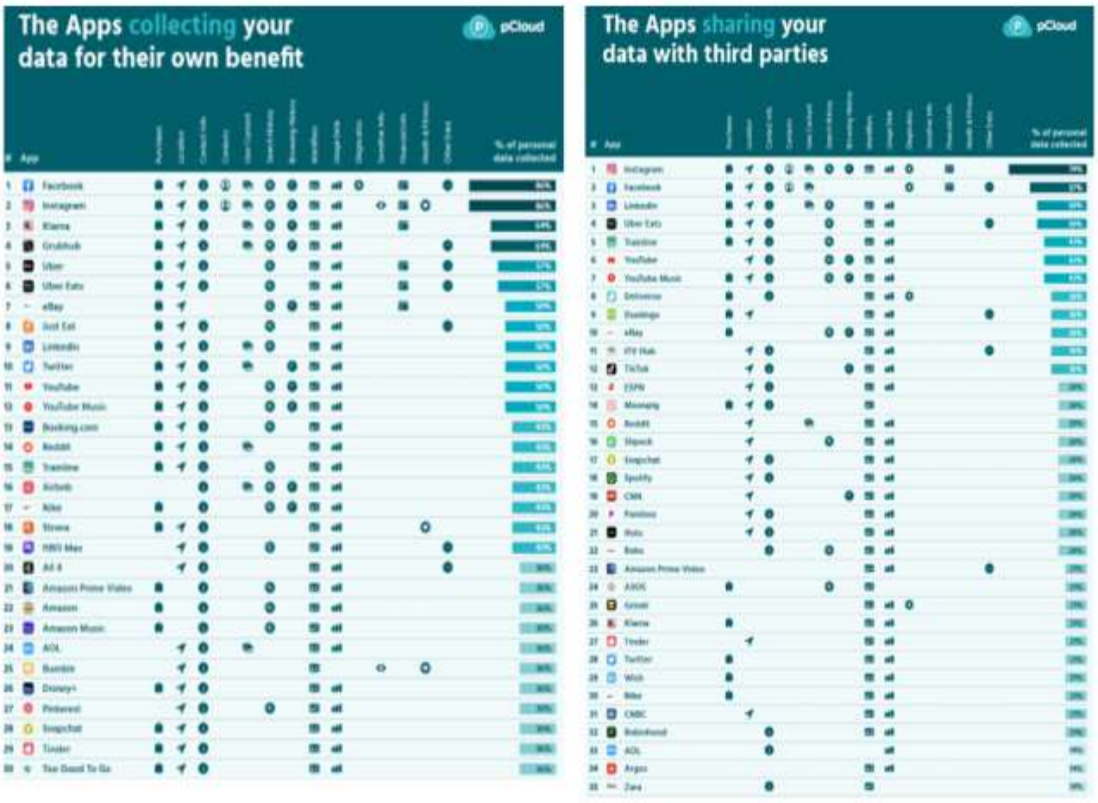


Figura 6[4]

Nella Figura 7 si possono vedere:

- uno stralcio della classifica delle 100 app più popolari nel mondo, stilata in ordine di invasività in termini di quantità di dati complessivamente

[4] https://blog.pcloud.com/invasive-apps/

raccolti e trattati per marketing interno e condivisione con terze parti: inaspettatamente, app come Amazon e Airbnb sono in fondo alla classifica (14%), mentre la parte del leone spetta a Instagram e Facebook;
- e anche la classifica delle app più virtuose.

Figura 7[5]

1. Gli esordi della disciplina di riferimento per il marketing comportamentale: i rischi

Già alla fine degli anni '90 – nel vigore della Dir. 95/46/CE sulla protezione dei dati personali e della Dir 97/66/CE sulla tutela della vita privata nel settore delle telecomunicazioni – il WP29 mostrava con chiarezza quali fossero i punti focali della problematica: la Racc. 1/99 evidenziava l'uso, già allora invalso, di tecniche di "clicktrails" – che si attuavano, all'insaputa dell'utente [6], mediante cookies di utenti internet identificati o identificabili – e ne deduceva la necessità di:

- stimolare una configurazione dei software che non consentisse il trattamento di default di informazioni persistenti dell'utente, lasciando invece all'utente stesso di scegliere sempre (i) "*se accettare o respingere la trasmissione o la memorizzazione di un cookie nel suo insieme*"; (ii) eliminare selettivamente informazioni "*in modo semplice e senza*

[5] https://blog.pcloud.com/invasive-apps/
[6] Sulla mancanza di trasparenza della raccolta di dati effettuata in occasione della navigazione Internet, cfr. M. Viggiano, *«Navigazione» in internet e acquisizione occulta di dati personali*, Dir. Inf., 2007, II, 388; sul carattere occulto delle tecniche di profilazione online si veda anche A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa,* Milano, 2007, spec. 167 ss. e le opere ivi richiamate.

(necessità della) *partecipazione del mittente*" del marcatore;
- informare l'utente in modo trasparente e comprensibile su "*quali informazioni s'intendono memorizzare nel cookie, ed a quale fine, nonché il periodo di validità del cookie stesso*".[7]

Nei primi anni 2000 poi il WP29 [8] sollevava specificamente anche altri aspetti più specifici: prima il tema della rilevazione di dati personali effettuata tramite pseudonimi o numeri di identificazione non personalizzati e poi le caratteristiche di nuovi strumenti (il protocollo – allora nuovo – IPv6) [9] che, integrando un identificativo esclusivo nell'indirizzo IP del dispositivo, consentivano con sicurezza il collegamento tra loro di tutte le comunicazioni dell'utente che usa quel dispositivo.

Di conseguenza, già a quell'epoca il WP 29 identificava gli effetti di alto rischio per i dati personali e i diritti degli utenti che derivavano dell'uso di questi marcatori.

2. Gli esordi della disciplina di riferimento per il marketing comportamentale: le misure per mitigare il rischio.

Le conclusioni allora raggiunte quanto ai mezzi per mitigare questi rischi risultano tuttora estremamente attuali; quanto ai singoli siti, già allora il WP29 innanzitutto:

- chiedeva di adottare l'uso di meccanismi basati "perlomeno" sul diritto di opposizione al trattamento e comunque sul consenso informato e revocabile per la profilazione, prevedendo già la formula della finestra pop-up [10], e comunque capaci di garantire i diritti, oltre che di opposizione, anche di accesso, rettifica, cancellazione (anche selettiva) dei dati
- e dettava [11] gli elementi minimi dell'informativa, individuando obblighi informativi puntuali sia nell'oggetto (obbligo di fornire informazioni su tipo di dati raccolti, ambito di utilizzo e periodo di memorizzazione, nonché sulle finalità del trattamento, compresa la eventuale comunicazione a terzi) sia nella forma: anche questa raccomandazione già prevedeva l'uso del banner (casella prompt), da attivare a prescindere

[7] WP17 – RACC. 1/1999 sul trattamento invisibile e automatico dei dati personali su Internet. In dottrina, sulla progressiva patrimonializzazione dell'informazione e l'evoluzione della normativa a protezione dei dati personali, cfr. A. Mantelero, *Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies,* in Dir. Inf, Vol. XXVIII, p. 781, 2012; Id. *Il costo della privacy tra valore della persona e ragione d'impresa,* cit. 171 ss.

[8] Cfr. doc. di lavoro WP37 sulla "*Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line*", adottato il 21 novembre 2000, in cui – nel contesto di una disamina di più di 100 pagine sugli aspetti tecnici di Internet e di specifici servizi (es. posta elettronica, chat, forum di discussione, pagamenti elettronici, browser, world wide web…), si analizzano sotto il profilo giuridico gli aspetti di rischio per la vita privata, anche in tema di "cybermarketing": «*Queste informazioni devono essere fornite anche nei casi in cui i dati vengano rilevati usando pseudonimi o numeri di identificazione non personalizzati.*". Sul tema si veda anche WP28 – Op. 1/2000 su alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali.

[9] Cfr. il parere WP37 2/2002 "*sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6*".

[10] Cfr. WP43 – RACC. 17/5/2001 relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione Europea, par. 2.2, par. 16, ma anche WP37, cit.

[11] Racc. 1/1999, cit.

dalla capacità del browser di riconoscere e notificare all'utente il deposito del cookie.

Ma non solo: nella individuazione delle possibili azioni di mitigazione del rischio il WP29 assumeva anche un'ottica più generale, legata alle peculiarità di questo contesto in cui l'utente difficilmente percepisce ciò che accade e le conseguenze che possono verificarsi in termini di danno, e comunque raramente riesce ad agire di conseguenza in modo efficace, dovendo peraltro anche previamente identificare i responsabili.

Di conseguenza, il WP29 già all'epoca aveva:

a) sottolineato l'importanza dello sviluppo di tecnologie che "*migliorano, rispettano e sono conformi alla vita privata*", tra cui:
   – browser dotati di impostazioni predefinite in tale senso
   – strumenti di navigazione anonima
b) e auspicato azioni di sensibilizzazione degli utenti su questi temi e l'adozione di una norma europea per le certificazioni sulla "vita privata".

Merita veramente rilevare come sin dall'inizio le analisi condotte sul trattamento occulto di dati personali e informazioni attinenti alla vita delle persone collegato alla navigazione online abbiano constatato l'insufficienza della sola applicazione di strumenti basati sul consenso informato e la necessità – perché la protezione sia effettivamente garantita – dell'integrazione con tecnologie che siano conformi alle norme by design [12].

3. La normativa applicabile alle tecnologie di tracking online: le norme rilevanti.

Tutte le analisi, pareri, raccomandazioni sul tema sono poi confluiti nella Direttiva 2002/58/CE, nella cui applicazione ricade l'uso di tecnologie di tracciamento online, cookies e altri [13].

Questa Direttiva assume un ruolo integrativo (anche in senso interpretativo ed esplicativo) rispetto a quella generale sulla protezione dei dati personali, come risulta chiaro sin dal suo esordio [14].

Oggi la Dir. 95/46/CE è stata sostituita dal GDPR, ma ciò non inficia la fattibilità dell'azione comune tra le due normative, che anzi le nuove norme

---

[12] Sul ricorso a tecnologie conformate per consentire – in particolare nell'ambiente online - l'effettiva esplicazione del potere di controllo sui propri dati personali da parte dell'interessato, si veda A. Mantelero, *Digital privacy: tecnologie "conformate" e regole giuridiche*, in *Privacy digitale. Giuristi e informatici a confronto*, Torino, Giappichelli, 2005, 19 ss.
Non è questa la sede per approfondire l'argomento, ma merita rilevare che vi è da tempo ampia letteratura che osserva l'inidoneità di fatto del consenso a garantire tale controllo: *ex multis* cfr. S. Patti, *Il consenso dell'interessato al trattamento dei dati personali,* in *Riv. dir. civ.*, 1999, 467; L. Gatt, R. Montanari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di una riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2, 2017, 363 ss.; I. A. Caggiano, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, in Annali 2016-2018 – Università degli Studi Suor Orsola Benincasa; A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa,* cit., 304.

[13] Questione poi ripetutamente affrontata da WP29, Opp. 1/2008, n. 148 e 2/2010, n. 171 e recentemente dettagliata nel parere dell'EDPB 5/2019 sulle interazioni tra GDPR e Dir. e-Privacy.

[14] Cfr. l'articolo 1, comma 2, che indica come: *"(…) le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE*".

generali sulla protezione dei dati prevedono esplicitamente (art. 95 e cons. 173)[15], così come prevedono infine un riesame – attualmente ancora in corso [16]– della Dir. e-Privacy al fine di garantirne omogeneità col GDPR[17].

In quest'ottica è importante notare che, oltre all'aspetto programmatico, il GDPR risulta perfettamente coerente con una piena interazione delle due normative anche sotto il profilo dei contenuti specificamente relativi al contesto dell'uso di tecnologie di tracking online [18]: basta guardare il Cons. 30 del GDPR [19], che definisce gli identificativi online in modo perfettamente coerente con la Dir. e-privacy.

Figura 8

Come noto, il testo originario della Dir. e-Privacy ha poi subito modifiche nei punti d'interesse ad opera della Direttiva 136/2009, con previsioni infine

[15] GDPR Art. 95: "*Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE.*"; GDPR Cons. 173: "*È opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio, compresi gli obblighi del titolare del trattamento e i diritti delle persone fisiche.*".

[16] Proposta di Regolamento e-privacy del 10 febbraio 2021: il testo è oggetto del mandato negoziale del Consiglio d'Europa al Parlamento Europeo per la revisione definitiva.

[17] GDPR Cons. 173: "*Per chiarire il rapporto tra il presente regolamento e la direttiva 2002/58/CE, è opportuno modificare quest'ultima di conseguenza. Una volta adottato il presente regolamento, la direttiva 2002/58/CE dovrebbe essere riesaminata in particolare per assicurare la coerenza con il presente regolamento.*"

[18] EDPB – Op. 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities spec. par. 3.3.

[19] "*Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*".

recepite dall'Italia nel 2012 in legge (D. Lgs. del 28 maggio 2012, numeri 69 e 70), e che hanno anche aggiornato il Codice Privacy.

Allo stato, dunque, tra le norme rilevanti al fine della regolamentazione delle attività di trattamento effettuate tramite identificatori online in generale, e i cookies in particolare, si pone anche l'art. 122 del Codice Privacy.

4. Le norme rilevanti per le tecnologie di tracking online: i rispettivi campi di applicazione…

Il WP29 nel tempo si è impegnato a specificare il campo di applicazione di ciascuna delle normative rilevanti nel contesto in esame e le caratteristiche della loro interazione, espressa dall'art. 1 co. 2 della Dir. e-privacy.

In questo senso,

a) nell'Op. 2/2010 (WP 171)[20], aveva sintetizzato come:

- il quadro normativo dell'UE relativo all'uso dei cookie fosse costituito in via principale dall'articolo 5.3 della Dir. e-privacy, che si applica in ogni caso di "informazioni" archiviate o recuperate dall'apparecchiatura terminale di un utente di Internet, quindi anche quando non si tratti di dati personali, perché "*ciò che determina l'obbligo di cui all'art. 5 par. 3 è la protezione di un aspetto che si ritiene appartenente alla sfera privata dell'interessato, non il fatto che le informazioni siano o meno dati personali*"[21]
- la normativa generale (all'epoca, Direttiva 95/46/CE) si applicasse "*nei casi non specificamente coperti dalla direttiva e-privacy ogniqualvolta si procede al trattamento dei dati personali*"[22];

b) nella precedente Op. 1/2008 (WP 148)[23] aveva dettagliato gli estremi essenziali dell'interazione delle norme applicabili:

- precisando che l'art. 5 comma 3 della Dir. e-Privacy è una disposizione generale che si applica trasversalmente a tutti i servizi che fanno uso di tali tecniche (anche servizi non strettamente "di comunicazione elettronica", come i motori di ricerca),
- ricordando che l'art. 5.3 e il Cons. 25, nel regolare la conservazione di

[20] WP171 – Op. 2/2010 sulla pubblicità comportamentale online.

[21] Cfr. Op. 2/2010, cit., par. 3.2.1 e 6.1. Una piccola digressione: questa considerazione è particolarmente importante, e si ritrova costantemente rimarcata lungo tutta l'evoluzione del percorso di regolamentazione dei sistemi di tracciamento online, compresa l'attuale versione della proposta di Regolamento e-privacy, che precisa che "*Le apparecchiature terminali degli utenti finali di reti di comunicazione elettronica e tutte le informazioni relative all'uso di tali apparecchiature terminali, (…), fanno parte della sfera privata dell'utente finale* " e che "*Le informazioni raccolte dall'apparecchiatura terminale dell'utente finale possono spesso contenere dati personali.*" (cons. 20: "*Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, in particular where such information is processed by, stored in, or collected from such equipment, or where information is collected from it or processed in order to enable it to connect to another device and or network equipment, are part of the end-user's private sphere, including the privacy of one's communications, and require protection in accordance with the Charter of Fundamental Rights of the European Union.*" e in fine: "*The information collected from end-user's terminal equipment can often contain personal data.*").
Come vedremo anche esaminando alcune pronunce della Corte di Giustizia e ulteriori pareri dell'EDPB, è fondamentale tenere sempre presente che la protezione offerta dalla Direttiva (e poi dal Regolamento) opera oltre la categoria dei dati personali, andando a volte anche a derogare la normativa generale.

[22] Cfr. Op. 2/2010, cit., par. 3.1 e 6.1.

[23] WP148 – Op. 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca

cookie e analoghi dispositivi nel terminale di un utente, stabiliscono che ciò debba rispettare la normativa generale in tema di protezione dati personali

– e concludendo nel senso che dunque l'art. 5.3 chiarisce gli obblighi che in questo contesto (cioè, quanto alle tecnologie di tracking online) derivano dalla normativa generale.

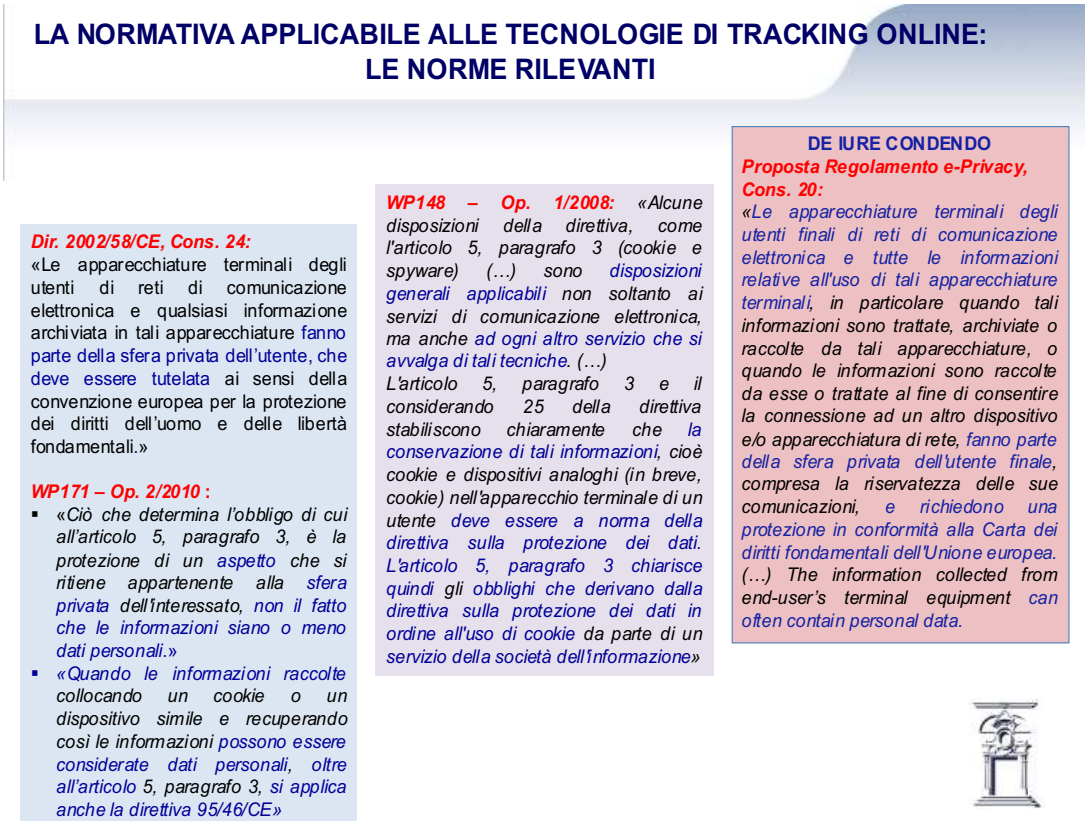


Figura 9

5. … e le regole di interazione.

Da ultimo, è intervenuto sul tema l'EDPB [24] con linee guida specificamente dedicate al tema della sovrapposizione e interazione della normativa generale sulla protezione dei dati con la Dir. e-privacy, in cui:

– ribadisce – a definitiva chiarezza – l'ambito di applicazione esteso dell'art. 5.3 della Dir. e-privacy, che si applica anche oltre il contesto dell'offerta di servizi di comunicazioni elettroniche, per cui anche agli editori di siti web o ad altre attività che fanno uso di cookies [25]

– ma soprattutto declina i meccanismi concreti della funzione integrativa che la Dir. e-Privacy è chiamata a svolgere nei confronti della normativa

[24] EDPB – Op. 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, cit.

[25] Par. 28: "*The overarching aim of the ePrivacy Directive is to ensure the protection of fundamental rights and freedoms of the public when they make use of electronic communication networks. In light of this aim, "articles 5(3) and 13 of the ePrivacy Directive apply to providers of electronic communication services as well as website operators (e.g. for cookies) or other businesses (e.g. for direct marketing).*"

generale a tutela dei dati personali, chiarendo cosa intenda il comma 2 dell'art. 1 della Dir. e-privacy quando recita: "*le disposizioni della presente direttiva precisano e integrano [particularise and complement] la direttiva 95/46/CE*".

Per fare questo assume come oggetto di analisi proprio l'uso di cookies, individuato quale trattamento di dati personali che tipicamente coinvolge entrambe le normative[26] e indica come i concetti di "precisare" (*particularise*) e "completare" (*complement*) debbano essere letti nell'ottica dell'applicazione del principio *lex specialis derogat legi generali*, e dunque:

- quando la Dir. e-Privacy regola in modo specifico, nel contesto di sua pertinenza, un trattamento di dati personali, allora essa prevarrà sulle previsioni generali di cui al GDPR [27]. Rispondono a questo principio anche i casi in cui le previsioni della Dir. e-privacy ampliano di fatto il campo di applicazione della normativa (ad esempio, l'estensione della protezione ad "abbonati" – oggi "contraenti" – e "utenti" di servizi di comunicazione elettronica, che possono anche essere persone non fisiche)[28]
- in tutti i casi in cui il trattamento coinvolga dati personali e non ci sia una previsione specifica della Dir. e-privacy, si applicherà invece il GDPR [29].

[26] Par. 29: "*There are many examples of processing activities which trigger the material scope of both the ePrivacy Directive and the GDPR. A clear example is the use of cookies.*".
Il fatto che quando le informazioni raccolte tramite cookies sono dati personali si applica anche la relativa normativa generale emerge peraltro anche da quanto già a suo tempo rilevato da WP171 – par. 3.2.2, pag. 10: "*Quando le informazioni raccolte collocando un cookie o un dispositivo simile e recuperando così le informazioni possono essere considerate dati personali, oltre all'articolo 5, paragrafo 3, si applica anche la direttiva 95/46/CE.*", nonché dalla più recente giurisprudenza della Corte di Giustizia in casi riguardanti trattamenti di dati personali effettuati mediante cookies: cfr. CJEU, C-210/16, 5 June 2018, C 210/16, ECLI:EU:C:2018:388, spec. para. 33-34. Si veda anche l'Opinion of Advocate General Bobek in Fashion ID, C-40/17, 19 December 2018, ECLI:EU:C:2018:1039, spec. para. 111-115.

[27] Si veda, al proposito, il par. 40 di EDPB – Op. 5/2019, nonché al par. 41, con l'esempio riportato, che evidenzia un possibile caso in cui l'art. 5.3 Dir. e-privacy, che prevede la base giuridica esclusiva del consenso per i cookies, prevale sulla previsione dell'applicabilità generale di basi giuridiche alternative di cui all'art. 6 GDPR.

[28] Questo ampliamento è confermato anche nella proposta di Regolamento e-privacy, che prevede l'applicazione delle norme agli "*user*" e, quanto al consenso, che "*The provisions for consent provided for under Regulation (EU) 2016/679/EU shall apply to natural persons and, mutatis mutandis, to legal persons*".

[29] Come confermato dal Cons. 173 GDPR: "*È opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio, compresi gli obblighi del titolare del trattamento e i diritti delle persone fisiche. Per chiarire il rapporto tra il presente regolamento e la direttiva 2002/58/CE, è opportuno modificare quest'ultima di conseguenza. Una volta adottato il presente regolamento, la direttiva 2002/58/CE dovrebbe essere riesaminata in particolare per assicurare la coerenza con il presente regolamento.*".

Figura 10

6. Tracking online e profilazione: quali basi giuridiche?

Come già detto, la Direttiva 2002/58/CE ha costituito il punto di arrivo sul tema di tutte le analisi, pareri e raccomandazioni degli anni che l'hanno preceduta.

Entrando nello specifico della base giuridica del trattamento di informazioni appartenenti alla sfera privata dell'utente (compresi i dati personali, ma non solo) effettuato tramite identificativi online, va ricordato che originariamente la Dir. e-privacy prevedeva la "*possibilità di rifiutare*" l'installazione del cookie: dunque, palesemente un consenso in forma passiva, di opt-out.

Soluzione che è stata modificata con la Dir. 136/2009, che ha introdotto la diversa richiesta di un consenso "*espresso preliminarmente*" (sempre con l'eccezione delle finalità tecniche).

Riferimento primario per queste indicazioni è stato il qui ripetutamente richiamato parere relativo alla pubblicità comportamentale on-line (WP 171), che nel 2010 aveva già tenuto conto (dichiarandolo esplicitamente) delle modifiche all'art. 5.3 Dir. e-privacy introdotte nel 2009, sebbene esse ancora non fossero state recepite dagli Stati membri (che avevano tempo per farlo fino al 2011).

In questo parere il WP29, in sede interpretativa dell'art. 5.3 della Dir., ha in particolare stabilito che il consenso:

a. deve essere ottenuto prima del collocamento del cookie o della raccolta delle informazioni archiviate nel terminale dell'utente ("*preliminarmente*");
b. deve essere espresso in modo conforme ai requisiti della normativa generale in materia di protezione dei dati personali.

Dunque, esaminando gli strumenti possibili:

B1. il consenso espresso mediante le impostazioni del browser

- non è conforme
  - se consiste nell'inattività dell'utente, nel caso in cui questi usi un browser che di default consente il trasferimento delle informazioni,
  - ma neppure "*se il browser è stato precedentemente impostato in modo tale da accettare tutti i cookie (…), in quanto, in generale, esso non può costituire una vera manifestazione di volontà dell'interessato*" perché "*non sarebbe né specifico né preliminare (al trattamento)*" [30] e neppure "informato", integrando così un consenso "di massa" a qualsiasi trattamento futuro, senza conoscenza delle relative circostanze.
- È invece conforme il consenso espresso mediante le impostazioni di browser che di default respingono i cookie di terzi **e** che impongono all'interessato di compiere un'azione positiva per accettare la collocazione e la continua trasmissione di informazioni contenute nei cookies.

Se i suddetti requisiti non sono soddisfatti, non basta certamente a integrare un consenso informato "*il fornire informazioni e, in una certa misura, il facilitare l'utente ad avvalersi della possibilità di respingere i cookie (spiegandogli il modo in cui procedere)*" [31].

B2. Non è conforme l'opt-out, che non presuppone alcuna partecipazione attiva perché in questa fattispecie l'intenzione dell'interessato è semplicemente presunta o implicita**.**

B3. È invece conforme il meccanismo di consenso opt-in [32] .

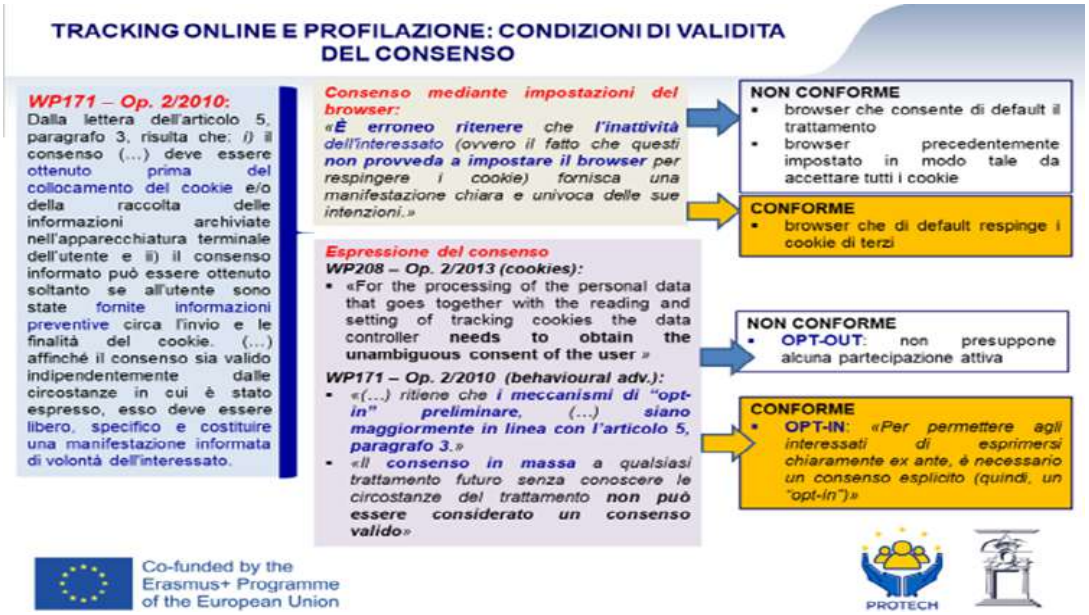


Figura 11

[30] WP 171, par. 4.1.1., lett. a), pag. 16

[31] WP 171, par. 4.1.1, pag. 17.

[32] WP 171, par. 4.1.3, pag. 18: "*Per permettere agli interessati di esprimersi chiaramente ex ante, prima cioè che avvenga il trattamento dei dati personali da parte di terzi, è necessario un consenso esplicito (quindi, un "opt-in") per tutte le operazioni di trattamento basate sul consenso*".

7. La portata del consenso.

Nell'ottica del processo tipico del marketing comportamentale, che coinvolge diversi attori / titolari del trattamento che operano per finalità proprie, la collocazione del cookie è prodromica a successivi trattamenti: dobbiamo dunque chiederci quale sia la portata del consenso ottenuto previamente all'installazione dei cookies.

L'Op. WP 171, anche tenendo esplicitamente in considerazione la difficoltà di ottenere in questo contesto consensi ripetuti, ha affrontato questo aspetto e, richiamando il tenore del Cons. 25 Dir. e-privacy[33], ha affermato che il consenso può essere ottenuto *in uno* per l'installazione del cookie e per la successiva raccolta di dati anche da parte dei siti partner di quello che ha installato il cookie [34], purché:

a) i cookie installati abbiano una durata limitata;
b) siano fornite informazioni in conformità alla normativa generale, tra cui:
   b1. la spiegazione sull'uso dei cookies per pubblicità mirata [35], da inserire in una finestra pop-up e non "affogata" nelle condizioni generali o nell'informativa privacy
   b2. una informazione periodica sul monitoraggio in corso [36] (perché le persone dopo un po' dimenticano i consensi che hanno dato): ad esempio, tramite la "*creazione di un simbolo e di messaggi associati che avvisino i consumatori del fatto che un fornitore di reti pubblicitarie sta monitorando il loro comportamento di navigazione al fine di trasmettere pubblicità mirata*" e che consenta la revoca del consenso;
c) il consenso sia liberamente e facilmente revocabile.

A questo proposito, il Garante, nelle recenti "Linee guida cookie e altri strumenti di tracciamento definitive, pubblicate il 9.7.2021,precisa che il gestore del sito web deve garantire la revoca del consenso "*in ogni momento e ciò in maniera semplice, immediata e intuitiva attraverso un'apposita area da rendere accessibile attraverso un link da posizionarsi nel footer del sito e che ne renda esplicita la funzionalità attraverso l'indicazione di "rivedi le tue scelte sui*

---

[33] "*25) L'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni".*

[34] Cfr. par. 4.1.3, pag. 18.

[35] Non sono sufficienti indicazioni generiche tipo: "inserzionisti e parti terze possono inoltre utilizzare i propri cookie o action tag").

[36] A questo proposito, segnalo che quest'obbligo è ripreso nella proposta di Regolamento e-privacy, all'art. 4°, comma 3: "*Agli utenti finali che hanno acconsentito al trattamento dei dati di comunicazione elettronica conformemente al presente regolamento viene ricordata la possibilità di ritirare il loro consenso a intervalli periodici di [non più di 12 mesi], finché il trattamento continua, a meno che l'utente finale non chieda di non ricevere tali promemoria*".
In proposito anche il nostro Garante, nelle sue recenti Linee guida cookie e altri strumenti di tracciamento definitive, pubblicate il 9.7.2021, ha (par. 6.2) stigmatizzato la diffusa "*ridondante e invasiva riproposizione*" del banner da parte dei gestori dei siti web e precisato che quando l'utente abbia liberamente scelto di non prestare il consenso, esso non dovrà essere nuovamente richiesto a meno che (i) siano cambiate le condizioni del trattamento o (ii) quando il gestore del sito web non possa sapere se un cookie sia stato già in precedenza memorizzato sul dispositivo: ad esempio, se l'utente sceglie di cancellare i cookie legittimamente installati nel proprio dispositivo e il titolare non abbia adottato altro sistema per tenere traccia del consenso espresso; oppure siano trascorsi almeno sei mesi dalla presentazione del banner all'utente.

cookie" o analoga": insomma, pur senza riproporre il banner la pagina iniziale del sito dovrà comunque rendere sempre disponibile il link alla privacy policy e all'area dedicata alle scelte granulari, tra cui i comandi per la revoca.

Naturalmente tutto ciò richiede un'attenta e aggiornata documentazione delle scelte dell'utente: a questo scopo, possono essere usati appositi cookie tecnici o comunque strumenti di tracciamento. Esistono ormai diverse piattaforme che offrono sistemi automatizzati di gestione dei cookies e alcune di queste consentono di tenere un "registro" aggiornato automaticamente in tempo reale dei consensi ricevuti e delle relative revoche.

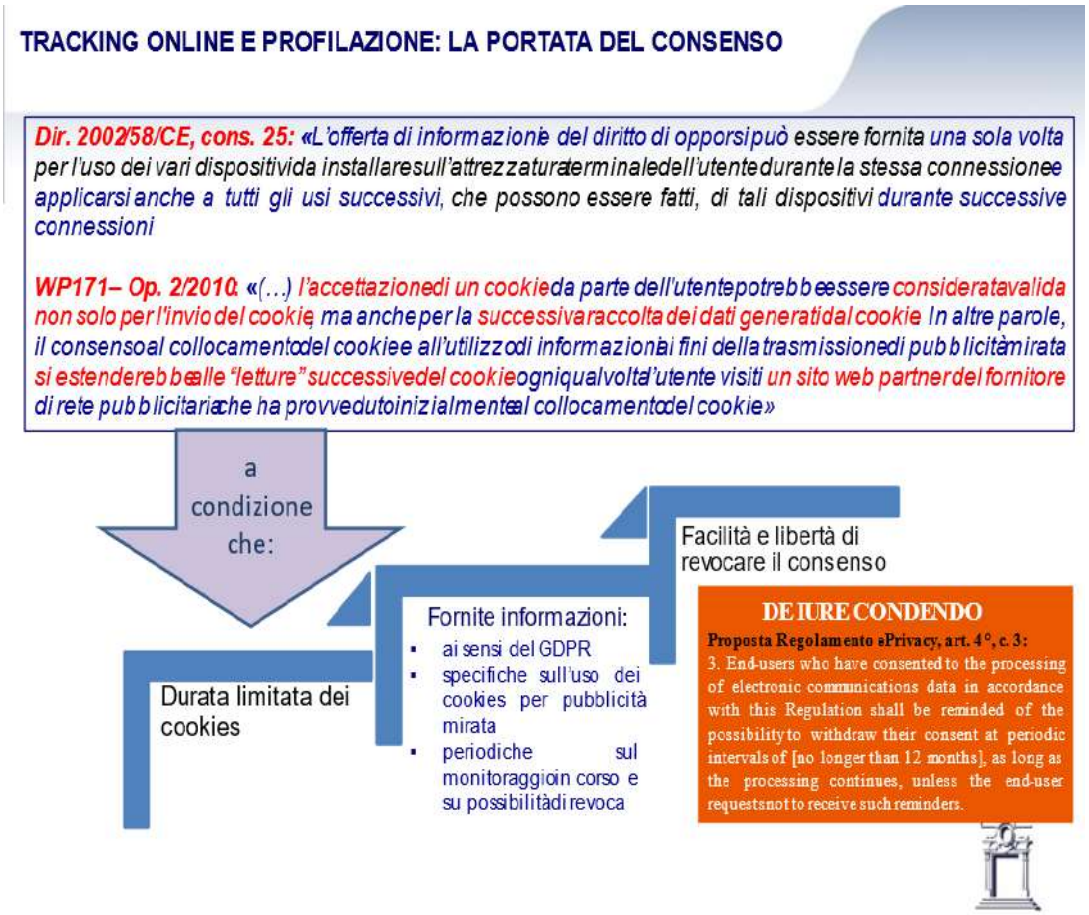


Figura 12

8. La ricerca di una visione paneuropea.

Negli anni successivi sono proliferate varie soluzioni pratiche individuate dagli operatori, variamente considerate dalle singole legislazioni e dalle DPA nazionali che a loro volta emettevano proprie linee guida (ad esempio, la legge svedese autorizzava addirittura l'obbligo di accettare i cookies per accedere al sito), finché nel 2013 il WP29 è nuovamente intervenuto in una visione di applicabilità pan-europea, tramite il working document WP208, a definire linee guida per ottenere un consenso valido ai fini specifici del trattamento

effettuato tramite identificativi univoci online.

Lo fa richiamando in toto quanto già detto nel 2010 (WP 171) e ribadendo e ulteriormente specificando gli elementi fondanti un valido consenso:

a) un'informativa specifica contenente informazioni appropriate (chiara, completa, visibile), posta in home page e visibile finché l'utente ha fatto la sua scelta, che indichi (anche con link):
   - le tipologie di cookies utilizzati, per finalità,
   - i terzi che possono avere accesso alle informazioni dell'utente,
   - durata,
   - dettagli su cookie di terze parti,
   - chiara specificazione di quali azioni manifestano il consenso e delle modalità per accettare o rifiutare l'installazione dei cookies, anche selettivamente, e revocare il consenso;

     a. raccolta del consenso preventiva al trattamento, ossia prima che i cookie siano installati o letti: dunque il sito deve utilizzare una forma di acquisizione del consenso priva di cookies;

     b. consenso consistente in una manifestazione di volontà attiva e inequivocabile: es click su un bottone o un link, su un'immagine o altri contenuti sulla home page, flag di un box, tramite impostazioni del browser solo alle condizioni indicate da WP171. Ciò che conta è che il contesto sia tale da rendere certa la volontà dell'utente. Non è valido a tale scopo il click su un link che offre ulteriori informazioni, così come l'inattività. Anche la pura permanenza sulla home page non è sufficiente;

     c. libertà e specificità del consenso: effettiva libertà di scegliere se accettare o meno i cookies, quali accettare o rifiutare e cambiare idea in futuro.

Un elemento integrante della libertà è la granularità del consenso, da definire sulla base delle finalità del trattamento: consentire di accettare o rifiutare selettivamente i cookies individuati per finalità garantisce la specificità del consenso.

Ciò è particolarmente importante anche per il rispetto dei principi di finalità, proporzionalità e non eccedenza: l'adozione di un meccanismo non granulare di accettazione dei cookies può indurre di fatto l'obbligo di accettare cookies non necessari per ottenere il servizio di interesse [37] (tanto più se tale servizio non può facilmente essere reperito altrove; ciò è stato rilevato accadere soprattutto nel settore pubblico).

[37] Cfr. EDPB, Guidelines 8/2020 v. 2.0, pag. 16: "*58. (…) Even if the processing of personal data is based on consent of the data subject, this would not legitimize targeting which is disproportionate or unfair.*"

Figura 13

9. Il consenso per i marcatori online: quali caratteristiche operative? Aspetti che possono essere considerati risolti.

Questo parere del WP29, che presupponeva a richiamava il contenuto dettagliato e preciso del precedente parere WP171, conteneva già le risposte definitive sulla gran parte delle azioni da intraprendere per un uso legittimo degli identificativi univoci online.

Da allora non ci sono state novità sostanziali, ma solo ripetuti chiarimenti, sempre più espliciti, tanto da parte del WP29 e poi dell'EDPB quanto della giurisprudenza della Corte di Giustizia e delle DPA nazionali.

Di seguito una sintesi almeno dei temi principali aperti nel tempo e delle risposte fornite, in alcuni casi ormai certe e definitive e in altri ancora in discussione.

- *Informazioni minime obbligatorie*: tipologia e finalità dei cookies, periodo di attività, accessibilità a terzi (le informative devono mettere l'utente in grado di identificare tutti i soggetti che possono trattare i suoi dati e le relative finalità in base al consenso che rilascia [38], dettagli su cookie di terze parti, modalità per esprimere il consenso, modalità di revoca del consenso.

  A proposito dei contenuti dell'informativa, è importante sottolineare che la proposta di Regolamento e-privacy [39] chiarisce ripetutamente la necessità di offrire all'utente, contemporaneamente al diritto di revocare il consenso ma in modo distinto, la specifica informazione della possibilità di opporsi al trattamento a fini di marketing, gratuitamente e

[38] In merito, si vedano *Corte Giust. C-673/17 Planet 49 Gmbh* e *Corte Giust. C-40/17 Fashion ID*, quest'ultima relativa al plugin Facebook. Si veda anche EDPB, Guidelines. 8/2020 v. 2.0, pag. 23 punto 75, che richiama EDPB Guidelines 05/2020 on consent under Regulation 2016/679, V.1.1, p. 16, punto 65.
[39] Cfr. art. 16, comma 6, lett. d).

offrendo modalità semplici ed efficaci.

- *Modalità per fornire l'informativa*: banner per le informazioni di base (tipologia di cookies e finalità) e link e pop-up (secondo livello) per le altre informazioni; il Garante suggerisce anche di sfruttare possibili modalità multichannel (canali video, interazioni vocali, assistenti virtuali, impiego del telefono, ricorso a chatbot…).
  Il Garante inoltre nelle sue linee guida ha riscontrato l'esistenza di un problema generale di assenza di codifica semantica uniforme dei cookie e degli altri sistemi di tracciamento, per cui – allo stato – non esiste modo di distinguere in modo obiettivo i cookie tecnici dagli analitici o di profilazione, dovendosi affidare unicamente a quanto dichiarato dai singoli titolari: ciò comporta la necessità che i titolari esplicitino nell'informativa o nella privacy policy i criteri di codifica adottati.
- *Forma del consenso*:
  - "soft opt-in" (preselezione) e opt-out: non sono ammessi, è necessaria un'azione positiva, che per le Autorità di protezione dei dati di Francia, Gran Bretagna, Germania, Belgio e Olanda deve esplicarsi nel click di un bottone o di un link specificamente riferito al consenso ai cookies;
  - lo scrolling fino alla fine del 2019 sembrava ancora ammesso dall'Autorità di protezione dei dati spagnola [40], e anche dal nostro Garante fino alla fine del 2020, sebbene già nel 2017 l'Art 29WP nelle sue linee guida sul consenso WP259 rev01 avesse chiarito che "*La semplice prosecuzione dell'uso normale di un sito web non è un comportamento dal quale si può dedurre una manifestazione di volontà dell'interessato a prestare il consenso a un trattamento proposto*".
    A tagliare la testa al toro ha pensato l'EDPB, che nelle Linee Guida 5/2020 sul consenso nel GDPR ha ribadito l'illegittimità di questo strumento ai fini del consenso, sulla base della considerazione del fatto che *"(…) azioni quali scorrere un sito o sfogliarne le pagine o azioni analoghe dell'utente non potranno in alcun caso soddisfare il requisito di un'azione positiva inequivocabile: azioni di questo tipo possono essere difficili da distinguere da altre azioni o interazioni dell'utente e quindi non è possibile stabilire che è stato ottenuto un consenso inequivocabile. Inoltre, in un caso del genere, sarà difficile dare all'utente la possibilità di revocare il consenso con la stessa facilità con cui lo ha espresso*." [41].
    Anche il Garante, nelle sue nuove linee guida [42] (par. 6.1), ha finalmente dichiarato che lo *scroll down*, o *scrolling*, sia di per sé totalmente inadatto a fungere da consenso, ma ipotizza comunque che possa assumere tale funzione ove inserito in un processo che per le sue caratteristiche complessive manifesti

[40] Cfr. le Linee guida AEPD del novembre 2019 e la decisione AEPD (Vueling) del 10/10/2019, in cui è ammessa l'equivalenza tra l'accettazione espressa da parte dell'utente dell'utilizzo dei cookie tecnici e di profilazione e la mera continuazione della navigazione. Questa posizione è stata modificata con l'aggiornamento del maggio 2020, a seguito delle linee guida dell'EDPB di cui alla nota che segue.
[41] EDPB, Guidelines 5/2020 on consent under Regulation 2016/679, es. 16, par. 86.
[42] Cit. nota 35.

un'azione positiva inequivoca dell'utente;

- *cookie walls e cookie barrier* (quest'ultima è la modalità per la quale il banner obbliga l'utente a scegliere se accettare o rifiutare i cookie, altrimenti non gli è consentito proseguire nella navigazione): anche su questo punto per lungo tempo non vi è stato accordo tra le Autorità di protezione dei dati, fino a quando con l'avvento delle linee guida EDPB 5/2020 è definitivamente emersa l'innegabile illiceità di questi strumenti di acquisizione del consenso [43]. Ciò, salva l'ipotesi (del tutto residuale, mi pare) che il gestore del sito sia in grado di offrire anche un'alternativa di navigazione/contenuto/servizio equivalente che sia priva di cookies.
  In considerazione del fatto che questa ipotesi – a suo tempo già avanzata dall'Art. 29WP nelle sue linee guida sul consenso WP259 del 2017 – è stata ripresa integralmente dall'EDPB e viene riproposta anche dal Garante nelle sue linee guida come opzione da valutare caso per caso, sembra necessario approfondire quali sono le circostanze rilevanti.
  Questo il ragionamento proposto dall'EDPB:
  "*37. Il titolare del trattamento potrebbe sostenere che la sua organizzazione offre all'interessato una scelta reale mettendolo in grado di scegliere tra un servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente che non implica un siffatto consenso, dall'altro.*
  Finché esiste la possibilità che il contratto venga eseguito, o che il servizio oggetto del contratto venga prestato, dal titolare del trattamento senza necessità di acconsentire ad usi ulteriori o supplementari dei dati in questione non si è in presenza di un servizio condizionato. Tuttavia, i due servizi devono essere effettivamente equivalenti.
  38. Il Comitato ritiene che il consenso non possa considerarsi prestato liberamente se il titolare del trattamento sostiene che esiste la possibilità di scegliere tra il suo servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente offerto da un altro titolare del trattamento, dall'altro. In tal caso la libertà di scelta dipenderebbe dagli altri operatori del mercato e dal fatto che l'interessato ritenga che i servizi offerti dall'altro titolare del trattamento siano effettivamente equivalenti. Ciò implicherebbe inoltre l'obbligo per i titolari del trattamento di monitorare gli sviluppi del mercato per garantire la continuità della validità del consenso per le rispettive attività di trattamento dei dati, in quanto un concorrente potrebbe successivamente modificare il servizio prestato.
  Pertanto, il ricorso a tale argomentazione significa che un consenso fondato sull'esistenza di un'opzione alternativa offerta da un terzo non è conforme al regolamento generale sulla protezione dei dati, e pertanto un prestatore di servizi non può impedire all'interessato di accedere a un servizio per il fatto che questi non ha prestato il proprio consenso."

[43] EDPB Guidelines 5/2020, punto 39: "*Affinché il consenso sia prestato liberamente, l'accesso ai servizi e alle funzionalità non deve essere subordinato al consenso dell'utente alla memorizzazione di informazioni o all'ottenimento dell'accesso a informazioni già memorizzate nell'apparecchiatura terminale dell'utente (i cosiddetti "cookie wall")*". In generale sullo scambio tra consenso e servizio si veda C. Angiolini, *A proposito del caso Orange Romania deciso dalla Corte di Giustizia dell'UE: il rapporto tra contratto e consenso al trattamento dei dati personali*, in NLCC, n. 1/2021.

Insomma, è chiaro che condizione necessaria (ma non sufficiente) perché il servizio sia equivalente è che sia offerto dal medesimo titolare [44].

- Consenso specifico [45]: non è ammessa per ottenere un valido consenso l'estensione indebita delle funzionalità (ad esempio, tramite l'uso delle condizioni contrattuali: condizioni generali di acquisto, abbonamento…). Corollario della specificità del consenso è la sua granularità [46]: è ammesso un consenso generale per tutte le finalità di installazione e uso dei cookies, ma accompagnato da uno strumento (link, ulteriori layer…) che dia la possibilità alternativa di esprimerlo in modo granulare per singola finalità;
- Consenso libero: ciò implica che la revoca o il rifiuto del consenso non comporti pregiudizi [47] di alcun tipo all'interessato.

Fig. 14

[44] Si vedano sul punto le riflessioni critiche di S. Thobani, in *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in MediaLaws 3/2019, 142. L'A., a supporto della rappresentazione del "consenso libero" quale consenso prestato a favore di un'alternativa, non rilevando se sia fornita da operatori terzi, richiama anche Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Giur. it.*, 3, 2019, 530 ss., che individua l'assenza di libertà nel consenso cui viene subordinata una prestazione "*ad un tempo infungibile e irrinunciabile per l'interessato*" (143).

[45] Cfr. EDPB 5/2020 par. 3.2, pag. 15, punto 56: *"(…) La necessità di un consenso specifico associata alla nozione di limitazione delle finalità di cui all'articolo 5, paragrafo 1, lettera b), funge da garanzia contro l'ampliamento progressivo, o la commistione, delle finalità di trattamento dei dati dopo che l'interessato ha acconsentito alla loro raccolta iniziale. Questo fenomeno, noto anche come "function creep", rappresenta un rischio per l'interessato, in quanto può comportare l'uso non previsto di dati personali da parte del titolare del trattamento o di terzi e la perdita del controllo da parte dell'interessato.*"

[46] Cfr. EDPB 5/2020 spec. par. 3.1.3.

[47] Cfr. EDPB 5/2020 spec. par. 3.1.4. Sulle possibili attribuzioni ed effetti del requisito di «libertà» del consenso, si veda – oltre alla dottrina e giurisprudenza citate in nota 44 – l'approfondita analisi di S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità,* in Europa e diritto privato - 2/2016, spec. 520 ss., e la ricca panoramica di dottrina ivi contenuta, che – benché si riferiscano alle norme del Codice Privacy ante GDPR – risultano, *mutatis mutandis*, ancora perfettamente attuali.

- Determinazione della base giuridica per l'inserimento del plug-in social in un sito:
  Il meccanismo del plugin è diverso dai cookies, sebbene operi mediante archiviazione di cookies nel terminale dell'utente; di base serve a consentire agli utenti dei social network di condividere contenuti a loro graditi con i loro "amici": in questo caso, rientra tra le esenzioni al consenso di cui alla seconda parte dell'art. 5.3 della Direttiva e-Privacy (che, si ricorda, fa riferimento all'archiviazione tecnica o accesso "*nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio*").
  Però in certi casi può anche essere utilizzato per altre finalità, ad esempio "*per monitorare gli individui, membri o meno* [del social network – n.d.r.]*, con cookie di terzi per finalità aggiuntive come, ad esempio, la pubblicità, l'analitica e le indagini di mercato a carattere comportamentale*" [48]: in tale caso, non opera l'esenzione e subentra l'obbligo di consenso.
  Un recente precedente è costituito dalla decisione della Corte di Giustizia Fashion ID, C-40/17, del 29/7/2019, che ha spiegato che nel caso dell'uso di plugin il Giudice deve previamente verificare se si possa ritenere che nel caso di specie il social network – fornitore del plugin – acceda, tramite l'uso di questo, a informazioni archiviate nel terminale dell'utente ai sensi della prima parte dell'art. 5.3 Dir. e-Privacy oppure se sia applicabile l'esenzione.
  Nel caso di Fashion ID, peraltro, la Corte ha evidenziato (par. 75 ss.) come – fatti salvi gli accertamenti da effettuarsi da parte del Giudice del rinvio – "dagli atti risulta che, avendo inserito sul suo sito Internet il pulsante «Mi piace» di Facebook, la Fashion ID sembra aver offerto la possibilità alla Facebook Ireland di ottenere dati personali dei visitatori del proprio sito Internet, possibilità concretizzatasi sin dal momento della consultazione di tale sito, e ciò indipendentemente dal fatto che essi siano o meno iscritti al social network o che abbiano cliccato sul pulsante « Mi piace» di Facebook o, ancora, che siano a conoscenza di una tale operazione."
  Da ciò la Corte ha dedotto che la finalità dell'inserimento del plugin "Mi piace" da parte del sito fosse di tipo promozionale (rendere i suoi prodotti più visibili su FB) ed avesse un parallelo effetto economicamente favorevole per il social fornitore del plugin, che in questo modo beneficia dei dati del visitatore del sito ospitante, trasferitigli appunto mediante il plugin (e dunque accedendo a informazioni – cookies – archiviate nel terminale dell'utente). Ricorre pertanto in questo caso la necessità del consenso.
  Peraltro, la Corte svolge anche interessanti valutazioni in tema di titolarità del trattamento, specificando come (parr. 64 ss.) l'editore del sito che inserisce sul suo sito il plugin social sia titolare solo dei trattamenti di raccolta dei dati personali dei visitatori del suo sito Internet e conseguente comunicazione, mediante trasmissione, al social,

[48] Cfr. Art. 29WP, Op. 4/2012 - WP 194, par. 4.1.

mentre non ha possibilità di determinare i trattamenti che il social fa dei dati così ricevuti. PERÒ, attenzione: il social è contitolare del trattamento dell'editore del sito per queste stesse finalità.
Ciò malgrado, è l'editore del sito il soggetto tenuto a fornire l'informativa e chiedere il consenso per le finalità di raccolta e comunicazione mediante trasmissione al social dei dati personali dei visitatori del suo sito Internet, "giacché è il fatto che un visitatore consulti tale sito Internet che attiva il processo di trattamento dei dati personali. (…) non sarebbe conforme a una tutela efficace e tempestiva dei diritti della persona interessata il fatto che il consenso sia prestato unicamente al corresponsabile del trattamento che interviene successivamente, ossia al fornitore di detto plug-in".
Tutto questo è stato poi confermato da EDPB Guidelines 8/2020 v. 2.0 sul targeting degli utenti di social media, – che ha sottolineato che: "(…) *il consenso che dovrebbe essere raccolto dal gestore del sito web per la trasmissione di dati personali attivata dal suo sito web (incorporando un plug-in sociale) si riferisce solo all'operazione o all'insieme di operazioni che comportano il trattamento di dati personali di cui il gestore determina effettivamente le finalità e i mezzi. La raccolta del consenso da parte del gestore di un sito web, non esclude né diminuisce in alcun modo l'obbligo del fornitore di social media di assicurarsi che l'interessato abbia fornito un consenso valido per il trattamento di cui è responsabile in qualità di contitolare del trattamento, nonché per qualsiasi trattamento successivo o ulteriore che effettua e per il quale il gestore del sito web non determina congiuntamente le finalità e i mezzi (ad esempio, le operazioni di profilazione successive a fini di targeting).*" [49]

Fig. 15

[49] Par. 5.3.2, pag. 21, mia traduzione.

10. Caratteristiche operative del consenso per i marcatori online: i problemi ancora aperti.

Naturalmente permangono anche temi su cui dubbi e contrasti non sono ancora del tutto sopiti.

Di seguito ne ricordo i principali.

- *Uso di cookies analytics: richiede il consenso?*

  Le Autorità di protezione dei dati sono ormai tutte abbastanza allineate in senso positivo, seppure con qualche differenza: ad esempio, la Germania chiede il consenso per il caso in cui l'uso degli analytics sia preordinato ad un trasferimento dei dati a terzi.

  In ogni caso, il WP29 già nel 2012[50] aveva specificato che gli analytics non sono necessari per erogare un servizio espressamente chiesto dall'utente, dunque non sono esentati dal consenso ai sensi della seconda parte dell'art. 5.3 della Direttiva e-Privacy.

  Aveva però anche osservato che gli analytics di prima parte che si limitino a formulare statistiche aggregate con completa anonimizzazione dell'indirizzo IP non sono pericolosi per la protezione dei dati personali, a condizione che siano attuate tutele ragionevoli, tra cui informazioni adeguate, la facile capacità di recesso e meccanismi di completa anonimizzazione di tutte le informazioni identificabili (tra cui l'indirizzo IP).

  A tali condizioni, quindi, sebbene a rigore non rientrino nell'esenzione di cui alla seconda parte dell'art. 5.3 della Direttiva e-Privacy, è possibile utilizzarli senza il consenso.

  Questa conclusione oggi è condivisa dal nostro Garante, che ha dato le seguenti indicazioni:

  - ha confermato la validità in questo senso del "mascheramento" di parte dell'indirizzo IP: "*La struttura del cookie analytics dovrà allora prevedere la possibilità che lo stesso cookie sia riferibile non soltanto ad uno, bensì a più dispositivi, in modo da creare una ragionevole incertezza sull'identità informatica del soggetto che lo riceve. Di regola questo effetto si ottiene mascherando opportune porzioni dell'indirizzo IP all'interno del cookie*";
  - ha escluso la liceità di qualsiasi combinazione con altre informazioni e trasferimenti a terzi: "*Resta inteso pertanto che i soggetti terzi, che forniscono al publisher il servizio di web measurement, non dovranno comunque combinare i dati, anche così minimizzati, con altre elaborazioni (file dei clienti o statistiche di visite ad altri siti, ad esempio) né trasmetterli a loro volta ad ulteriori terzi, pena l'inaccettabile incremento dei rischi di identificazione dell'utente; tranne il caso in cui la produzione di statistiche da loro effettuata con i dati minimizzati interessi più domini, siti web o app riconducibili al medesimo publisher o gruppo imprenditoriale.*"

[50] Cfr. WP29 Op. 4/2012 - WP 194, sull'esenzione dal consenso per l'uso di cookies, par. 4.3.

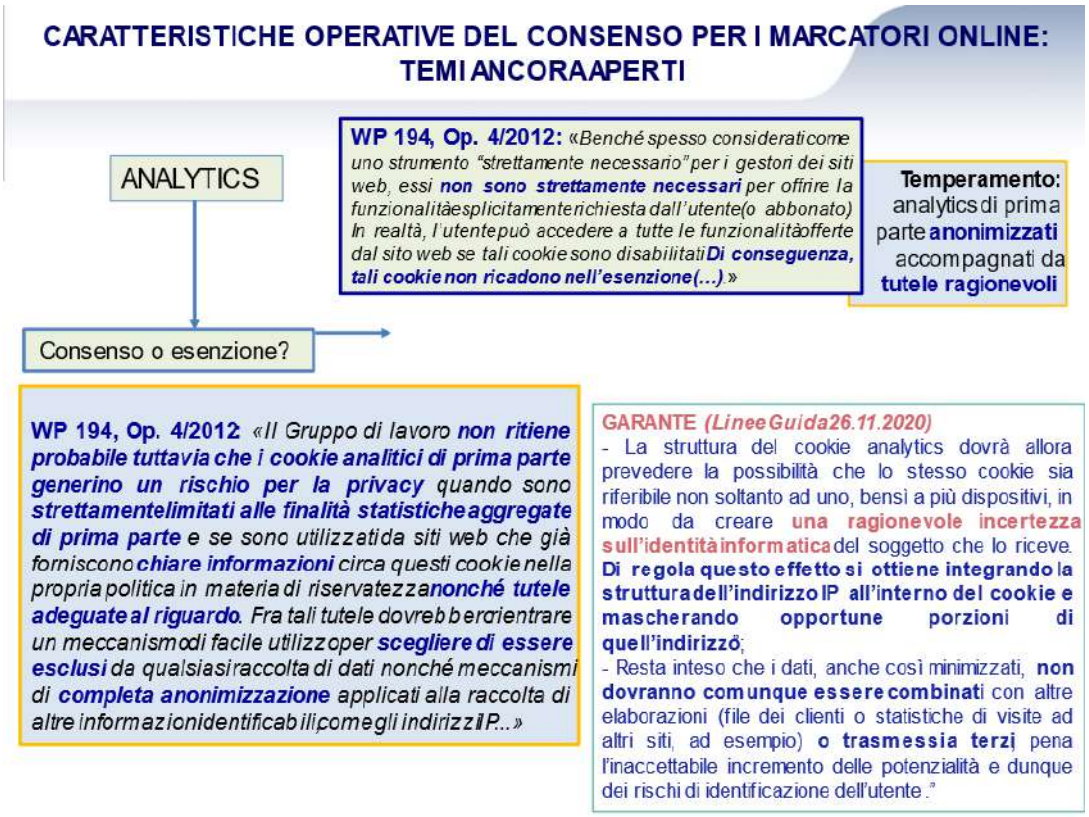


Fig. 16

Da ultimo, mi sembra utile affrontare brevemente l'interrogativo – che da qualche parte viene ancora posto – relativamente alla possibilità che ricorrano basi giuridiche diverse dal consenso in casi di trattamenti successivi all'installazione dei cookies (per esempio, la profilazione).

In particolare, sono sempre più numerosi i siti web che ricorrono all'interesse legittimo come base per questi trattamenti. Ad esempio:

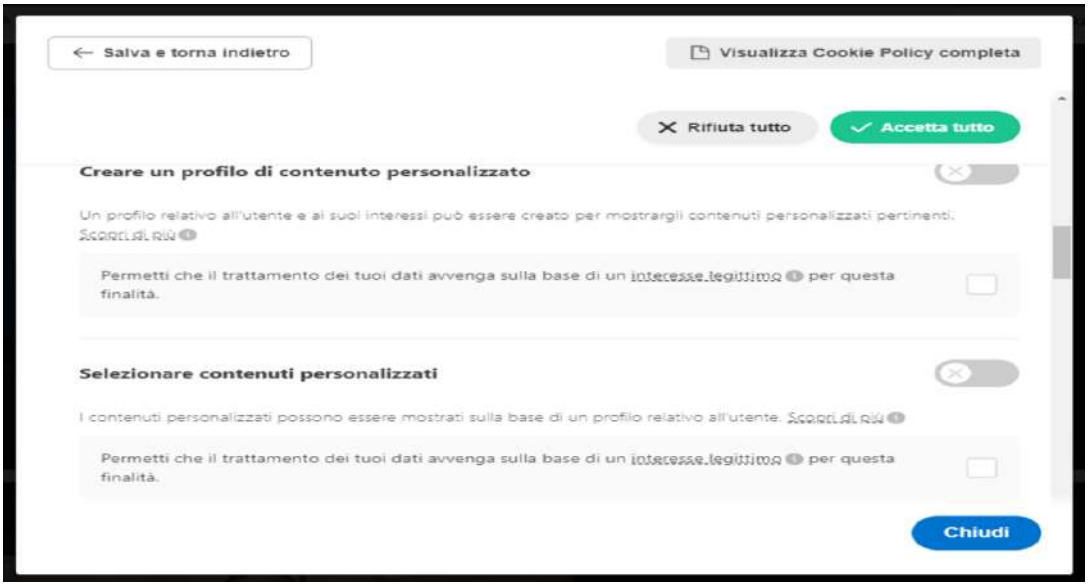


Fig. 17

Questa pratica deve ritenersi illegittima: vediamo perché.

- *Per i trattamenti successivi all'installazione dei cookies è lecito utilizzare basi giuridiche diverse dal consenso?*
  Il WP29 nell'Op. 2/2010 (par. 3.2.1) identificando il campo di applicazione materiale dell'art. 5.3 Direttiva e-Privacy nell'ottica proprio di individuare gli adempimenti per chi fa pubblicità comportamentale,
  - ha ricordato che l'art. 5.3 della Direttiva e-Privacy prevede il consenso per "l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente";
  - e ha quindi precisato che: "Considerato che (i) i tracking cookie sono "informazioni" archiviate nell'apparecchiatura terminale dell'interessato, e che (ii) i fornitori di reti pubblicitarie accedono a tali cookie quando l'interessato visita un sito web partner, l'articolo 5, paragrafo 3, trova piena applicazione.
    Pertanto, (…) qualsiasi successivo utilizzo di cookie precedentemente archiviati per accedere alle informazioni dell'interessato dovrà essere conforme all'articolo 5, paragrafo 3."

  Successivamente l'EDPB con l'Op. 5/2019
  - ha affermato (par. 75) che i (diversi) trattamenti successivi all'archiviazione o all'accesso alle informazioni ("all other processing operations that follow the storing of or access to information in the terminal device of the end-user") restano regolati dalla legge generale (e dunque, teoricamente potrebbero applicarsi basi giuridiche diverse dal consenso, ai sensi dell'art. 6 GDPR)
  - ma ha anche ricordato che i precedenti pareri WP sulla limitazione delle finalità (WP3/2013) e sul legittimo interesse (WP 6/2014) hanno richiamato il consenso attivo (opt-in) come unica legittima base giuridica per tutti i trattamenti a fini di marketing diretto o comportamentale e di profilazione basati su sistemi di tracking online (il WP 6/2014 richiamando peraltro direttamente l'applicabilità dell'art. 5.3 Dir.).

  Infine, l'EDPB ancora più recentemente, nell'Op. 8/2020 (par. 5.3.2)
  - ha riaffermato l'operatività dell'art. 5.3 della Direttiva e-Privacy in materia di requisiti per l'uso dei cookies, compreso ogni trattamento successivo dei dati personali ottenuti accedendo alle informazioni nel terminale e che "For what concerns the legal basis of the processing in Examples 4, 5, and 6, the EDPB considers that legitimate interest cannot act as an appropriate legal basis as the targeting relies on the monitoring of individuals' behavior across websites and locations using tracking technologies. 78. Therefore, in such circumstances, the appropriate legal basis for any subsequent processing under Article 6 GDPR is also likely to be the consent of the data subject." (par. 5.3.2, parr. 77-78, pag. 23 s.).

  È evidente da tempo, pertanto, la esclusione – secondo l'interpretazione del WP29 e quella conforme e complementare dell'EDPB –della ricorrenza di basi giuridiche differenti dal consenso per trattamenti

basati sull'uso di identificatori univoci online, anche successivi all'installazione dei marcatori.
Da ultimo, anche il nostro Garante Privacy, con le Linee guida cookie e altri strumenti di tracciamento pubblicate a luglio 2021

- ha precisato che *"(…) la disciplina di carattere speciale applicabile alla specie non contempla ulteriori basi giuridiche che rendano legittimo il trattamento se non in presenza del consenso dell'interessato ovvero al ricorrere di una delle ipotesi di deroga rispetto all'obbligo della sua raccolta previste proprio da tale disciplina speciale. In nessun caso sarà pertanto possibile invocare ad esempio, come è stato invece osservato nel corso delle verifiche effettuate su diversi siti web, la scriminante del legittimo interesse del titolare per giustificare il ricorso a cookie o altri strumenti di tracciamento."* (par. 5, ult. paragrafo, pag. 7).

Fig. 18

Credo poi che si debba anche considerare il fatto che la tutela apprestata dall'art. 5.3 non si applica solo ai dati personali, ma a tutte le "informazioni" dell'utente archiviate nell'apparecchiatura terminale, che sono considerate comunque afferenti tutte alla sua sfera privata, come da ultimo sottolineato anche dalla proposta di Regolamento e-Privacy (cons. 20)[51], che dichiara

[51] Cons. 20 della proposta Regolamento e-Privacy (v. nota 36): "*Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. (…) Therefore, the use of processing and storage capabilities and the collection of information from end-user's terminal equipment should be allowed only with the end-user's consent*

fermamente che proprio a causa della tipologia di informazioni archiviate o trattate dagli apparati, potenzialmente rivelatrici dei dettagli più intimi della vita e della personalità dell'utilizzatore, tutte queste informazioni meritano una protezione rafforzata.

E – aggiunge – tra queste informazioni possono essere presenti anche dati personali.

Mi sembra dunque che non avrebbe senso logico, né giuridico, creare due differenti percorsi di protezione quando la *ratio* della normativa è quella di difendere l'utente da tutte le attività di marketing comportamentale (profilazione compresa) che coinvolgono informazioni che lo riguardano raccolte e trattate nel contesto dell'uso di "*tutte le tecnologie basate sul principio dell'archiviazione e dell'accesso a informazioni sull'apparecchiatura terminale dell'utente*" [52].

Da ultimo, neppure mi pare che possa essere invocata in senso contrario la decisione della Corte di Giustizia C-40/17 Fashion ID, che si è preoccupata di valutare l'applicabilità del legittimo interesse[53].

L'approfondimento sull'applicabilità del legittimo interesse, infatti, in quella sede è stato condotto doverosamente sul presupposto del fatto (indicato dalla decisione come rilevato dal Giudice del rinvio) che in quella specifica circostanza il trattamento non aveva coinvolto solo informazioni archiviate nell'apparecchiatura terminale degli utenti, ma anche altri dati personali. È dunque al trattamento di questi dati che eventualmente potrebbe essere applicato il legittimo interesse: solo per questo, e in relazione solo a questo, la Corte ha ritenuto rilevante analizzare la questione.

Fig. 19

and or for other specific and transparent purposes as laid down in this Regulation. The information collected from end-user's terminal equipment can often contain personal data".

[52] WP29, Op. 2/2010, par. 2.2.

[53] Cfr. par. 87 ss.

11. Verso un marketing digitale senza third party cookies.

Negli ultimi anni, reagendo all'attenzione sempre maggiore manifestata dagli utenti rispetto all'uso dei propri dati personali, sempre più operatori hanno deciso di eliminare dai propri browser i cookie di terza parte. Già oggi i browser che impediscono l'uso di cookie di terza parte detengono circa il 29% di market share in Italia[54].

Firefox, Safari e anche Edge di Microsoft hanno nel tempo avviato azioni in questo senso:

- Firefox ha stabilito come modalità predefinita il blocco di tutti i cookie di terze parti e di tutte le eventuali attività di cryptomining con l'attivazione di default della funzione "enhanced tracking protection", praticamente invisibile all'utente, il quale si accorge del suo funzionamento solo quando visita un sito e vede l'icona di uno scudo nella barra degli indirizzi accanto all'URL, insieme a una piccola icona 'i' a dimostrazione che Firefox "*sta bloccando l'accesso di migliaia di società alle sue attività online*".
- Safari ha limitato il monitoraggio dei cookie dal 2017, utilizzando algoritmi di apprendimento automatico per identificare i comportamenti di tracciamento, come i cookie persistenti provenienti da reti pubblicitarie di terze parti.
- Edge prevede nella sua nuova versione tre profili preimpostati in base ai permessi concessi: "Di base", "Bilanciato" e "Rigido", che è possibile personalizzare: le autorizzazioni concesse ai siti, così come le notifiche ma anche i cookie di terze parti, comprendono anche il controllo del microfono e della fotocamera e la possibilità di essere avvisati se un sito desidera accedere al testo e alle immagini copiati negli appunti.

L'ultimo è Google, che già dal 2019 ha annunciato l'intenzione di bloccare i third-party cookie su Chrome a partire dal 2022, nel contesto di un progetto che ha chiamato "privacy Sandbox"[55]: in pratica viene creata una sandbox (un ambiente isolato) del browser, non accessibile agli inserzionisti, e qui i segnali registrati dai cookies, come clic o conversioni, vengono archiviati e misurati con metodi di machine learning che applicano misure di limitazione, offuscamento e anonimizzazione prima che i dati vengano restituiti.

L'algoritmo dunque segue la navigazione dell'utente e sulla base delle preferenze di navigazione lo inserisce in un grande gruppo di utenti aventi interessi simili, conservato nel sandbox e a cui poi mostra gli annunci dei terzi ritenuti appropriati.

In sostanza Google, tramite Chrome, non identificherà più l'utente con l'identificatore univoco personale salvato nei cookie e richiamato dai siti web terzi (anzi, l'ID verrebbe dissimulato), ma ne salverà le preferenze: dunque, la profilazione avviene lo stesso, ma senza più possibilità di individuare lo specifico utente.

---

[54] Dati del Politecnico di Milano – Osservatorio Internet Media – presentati il 9/3/2021 nel contesto della ricerca "Internet advertising: no cookie, no party" (accesso limitato agli abbonati). La presentazione La ricerca ha anche evidenziato come, con la realizzazione della "privacy sandbox" di Google Chrome la quota di mercato detenuta dai browser con limitazioni all'uso dei cookies salirà al 96% (Chrome da solo detiene il 67%).

[55] https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/ .

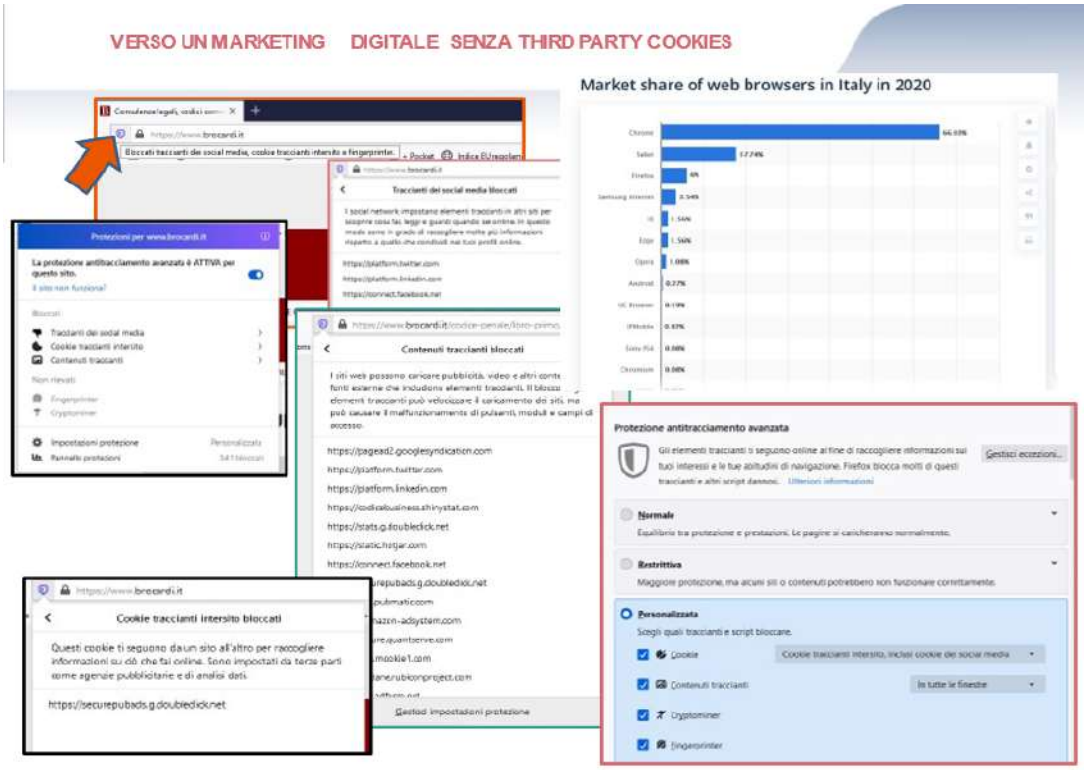


Fig. 20

È importante sottolineare ancora che quando si parla di un futuro senza cookie si fa riferimento al blocco da parte dei browser dei third party cookie (cioè creati da domini differenti da quello in cui si sta navigando), utilizzati per il tracciamento cross-site, il retargeting, la profilazione dell'utente e il matching degli ID degli utenti tra diverse piattaforme.

Per valutare gli impatti sul mercato di questo mutamento radicale va tenuto presente che Google controlla i due terzi del mercato e gestisce la più grande rete pubblicitaria su internet: DoubleClick (piattaforma di advertising che quando l'utente visita un dato sito rilascia i cookies che permettono di ricordare che quell'utente ha visitato quel dato sito) è il più grande fornitore di tecnologia pubblicitaria per editori e inserzionisti. E Google Analytics raccoglie informazioni da milioni di siti Web…

Quello che è chiamato Programmatic Advertising (il marketing basato sulla sincronizzazione dei cookies che consente di tracciare cross-site l'utente, profilarlo e veicolargli al momento giusto l'annuncio adatto) negli anni ha aumentato il suo peso all'interno dell'industry pubblicitaria proprio grazie alle sue alte potenzialità di targetizzazione: secondo l'Osservatorio Internet Media del Politecnico di Milano, ha raggiunto nel 2020 il valore di 588 milioni di euro in Italia, in crescita del 6% rispetto al 2019.

Per questo la decisione di Google di abbandonare i cookie di terza parte potrà generare conseguenze veramente importanti per tutto l'ecosistema di marketing e comunicazione, che negli ultimi anni ne ha fatto larghissimo utilizzo.

È importante considerare che il blocco dei cookie di terza parte non avrà impatti solo sulla delivery degli annunci e la targetizzazione degli utenti, ma ci

saranno conseguenze anche per quanto riguarda l'ambito della misurazione delle campagne online: ad esempio, sarà molto difficile ricostruire il percorso di navigazione dell'utente per l'impossibilità di individuare gli accessi precedenti effettuati con browser e device diversi, e quindi impossibile sapere cosa ha portato ad un determinato click e come interpretare il significato di una determinata conversione (vendita). Si presume che interverranno sempre più logiche di machine learning, che sostituiranno i modelli probabilistici al tracciamento diretto dell'utente.

Nel report dell'Osservatorio Internet Media del Politecnico di Milano (pag. 3) si legge: "*Solo gli Over The Top, almeno in questa fase, verranno toccati marginalmente, tanto che probabilmente rafforzeranno ancora il loro ruolo e peso all'interno del panorama pubblicitario. Grazie ai loro ecosistemi walled garden* [ossia caratterizzati da un parco di utenti registrati, loggati, con cui hanno un rapporto diretto e da cui traggono informazioni di prima mano, anche usando di cookie di prima parte – n.d.r.] *potranno utilizzare all'interno di questi ambienti (chiusi) l'ampia quantità di dati in loro possesso, ovviamente anche per fini pubblicitari. Il rapporto di forza degli OTT rispetto agli editori online potrà forse ridursi se i publisher, in un futuro prossimo, saranno in grado di organizzarsi con una "soluzione unica di sistema" in grado di rafforzare il proprio peso sul mercato e proporsi quindi come reale alternativa.*".

Si prevede quindi un impatto veramente importante se gli operatori, specie le aziende brand e anche gli editori online, non si attrezzeranno per trovare soluzioni alternative.

In quest'ottica, ciò che emerge dalla ricerca dell'Osservatorio Internet Media del Politecnico di Milano è la previsione del fatto che *"(…) oltre all'accelerazione verso il digitale indotta dalla pandemia, l'avvento dello "scenario cookieless" stimolerà ulteriormente in tutte le aziende (della domanda e dell'offerta) un forte senso di urgenza verso una cultura più matura del dato e della sua gestione.*", con l'assunzione di una rilevanza sempre maggiore:

- dei cookie di prima parte – che non sono impattati da queste evoluzioni dei browser –
- e dei dati acquisiti direttamente, con o senza meccanismi di tracciamento, magari ampliando il novero delle richieste di registrazione ai siti, alle newsletter, in modo da arricchire sempre più i sistemi CRM aziendali. In questo contesto, un ruolo particolare potrebbe essere assunto dall'indirizzo e-mail, che viene già raccolto con il consenso e cui vi è la possibilità tecnica di agganciare meccanismi che costituiscono veicolo di informazioni su azioni compiute dall'utente (es. apertura, cancellazione, attivazione di immagini all'interno mediante click…).

Ciò presumibilmente spingerà gli operatori verso l'introduzione di strategie e strumenti di marketing capaci di creare con gli utenti/interessati rapporti diretti e leali, destinati a durare e rafforzarsi nel tempo; ma, al di là della capacità di ridefinizione delle strategie di comunicazione che sapranno mostrare gli operatori, per il momento l'effetto più evidente e concreto resta quello che tramite la realizzazione della Privacy Sandbox Google si avvii ad un prossimo ulteriore e repentino rafforzamento della propria posizione di

mercato, idonea a distorcere pericolosamente la concorrenza[56].

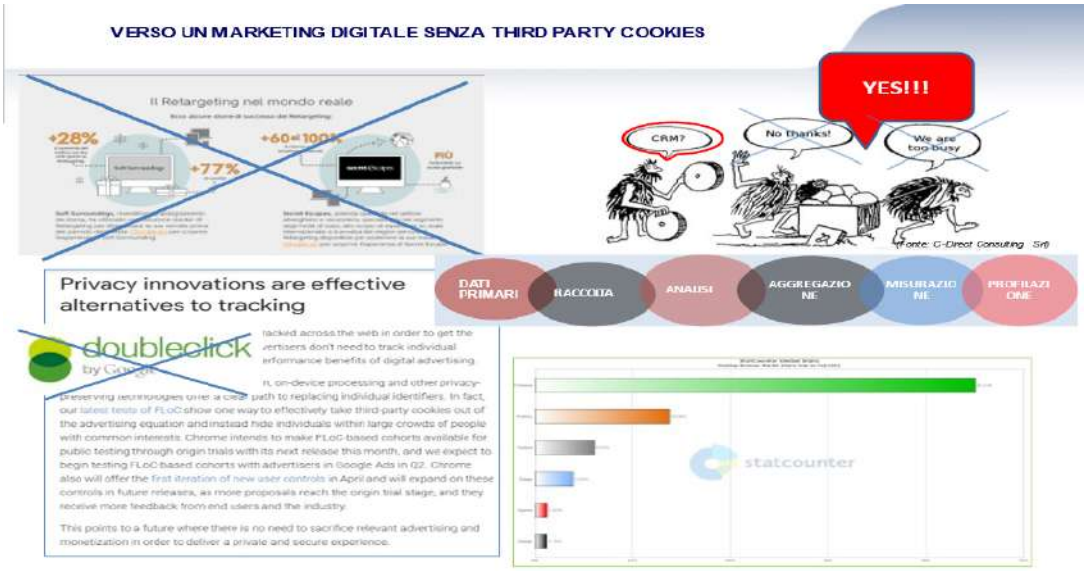
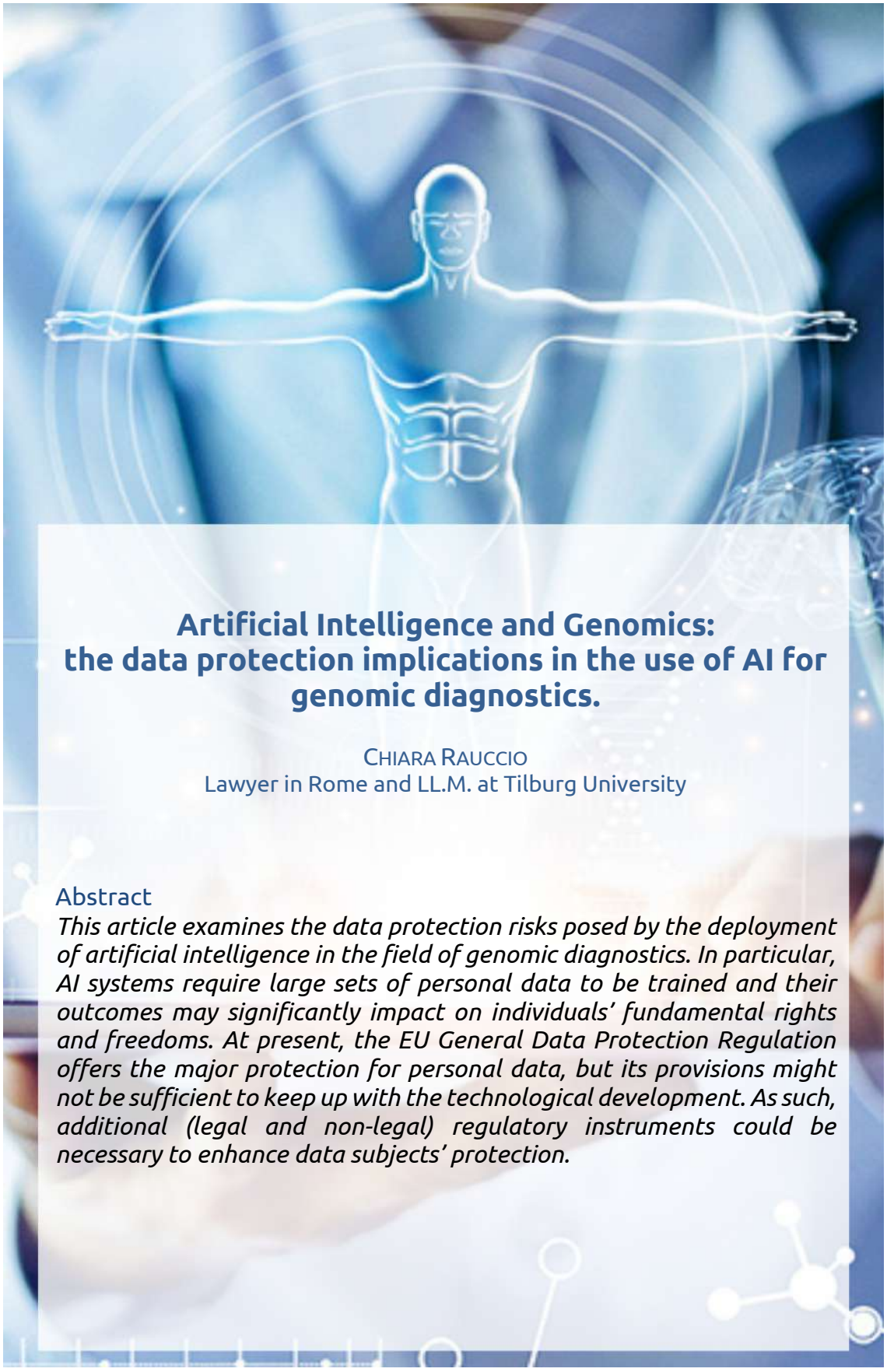


Fig. 21

[56] L'8 gennaio 2021 la Competition and Markets Authority (CMA), sollecitata da operatori del mercato, ha aperto un procedimento nei confronti di Google proprio con riferimento alla rimozione dei cookie di terze parti e altre funzionalità da Chrome. Attualmente Google ha proposto impegni, che includono tra l'altro limiti specifici su come Google può utilizzare e combinare i dati dei clienti per la pubblicità digitale, la cui idoneità a tutelare la concorrenza sul mercato della pubblicità digitale e contestualmente salvaguardare i dati personali degli utenti e stata oggetto di consultazione da parte di CMA e ICO e delle terze parti interessate; la consultazione si è chiusa l'8 luglio 2021 e allo stato l'Autorità sta valutando possibili modifiche agli impegni proposti da Google.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012



Artificial Intelligence and Genomics: the data protection implications in the use of AI for genomic diagnostics.

CHIARA RAUCCIO
Lawyer in Rome and LL.M. at Tilburg University

Abstract

This article examines the data protection risks posed by the deployment of artificial intelligence in the field of genomic diagnostics. In particular, AI systems require large sets of personal data to be trained and their outcomes may significantly impact on individuals' fundamental rights and freedoms. At present, the EU General Data Protection Regulation offers the major protection for personal data, but its provisions might not be sufficient to keep up with the technological development. As such, additional (legal and non-legal) regulatory instruments could be necessary to enhance data subjects' protection.

Keywords: data protection; artificial intelligence; machine learning; healthcare; genomic diagnostics; GDPR; soft law; ethics.

Introduction.

In the last few years artificial intelligence (AI)[1] has been increasingly applied in healthcare with the consequence to transform several aspects of medical practice and the potential to create new opportunities for patients' care, from more precise diagnosis and treatment applications (i.e. precision medicine)[2] to robotic assistance to caregivers, support for elderly care, and monitoring of patients' conditions.

An important field where AI will likely be deployed in the next years is genomic diagnostics, the branch of medicine which studies the interaction between disease and human genes and that finds its roots in genetic science. Genetics studies the structure of DNA and the functioning of genes (fragments of DNA that dictate the production of proteins). [3] The complete set of genes in a human being constitutes the "human genome" that encodes the genetic information and differs from individual to individual. Disorders and mutations of genes, combined with external factors like diet, lifestyle, and environment, may cause diseases. Genetic testing is used to ascertain whether a person has a genetic predisposition to developing a certain disease, or to confirm a diagnosis.[4] Yet, the development of a disease depends not only on genes, but

[1] For the purpose of this introduction the term "artificial intelligence" will be used as a generic reference to any computer systems intended to simulate human intelligence and human skills such as learning and problem-solving.

[2] D Cirillo, A Valencia, 'Big data analytics for personalized medicine' (2019) 58 Current Opinion in Biotechnology 161-167. See also the REVOLVER (Repeated Evolution of Cancer) project: https://www.healtheuropa.eu/personalised-cancer- treatment/87958/, or the Murab project which conducts more accurate biopsies, and which aims at diagnosing cancer and other illnesses faster: https://ec.europa.eu/digital-single-market/en/news/murab-eu-funded-project-success-story.

[3] It is based on the studies of genetics initiated in 1953 by Crick and Watson (see JD Watson, FHC Crick, 'Molecular Structure of Nucleic Acids: A Structure for Deoxyribose Nucleic Acid' (1953) Nature 737) who discovered that DNA is structured in a double helix constituted of genes that form the "human genome", a sequence of genes encoding the entirety of the genetic information stored in each cell and passed from each generation. In simple words, DNA is a string of complex molecules called nucleotides. It contains the genetic information of the individual in the form of instructions for building the molecules that make the body work (like proteins). Genes are segments of DNA that each carry a specific set of instructions for how to make a certain aspect of the individual (our genetic code contains around 23,000 genes). A genome is the complete set of the genetic material in an organism. For further details see https://scienceblog.cancerresearchuk.org/2018/05/29/science-surgery-whats-the-difference-between-the-words-genome-gene-and-chromosome/.

[4] PS Harper, 'What Do We Mean by Genetic Testing?' (1997) 34 Journal of Medical Genetics, 749.

on a variety of internal and external factors. Hence, traditional genetic tests can only provide an estimation of the risk to develop that disease.[5]

In this respect, AI may enhance diagnostic tools. Indeed, its capacity to analyse large amounts of data, identify correlations and generate inferences, as it will be explained in the next paragraphs, may enable more accurate predictions and thus earlier diagnosis and more effective treatments.

To properly work AI systems need to process large amounts of personal data related not only to health *stricto sensu,* but also to environmental and social aspects (e.g. economic status, air pollution levels, living place, job, eating habits).[6] Such data is combined into complex datasets and is analysed to create profiles to predict whether patients will likely develop a particular disease.[7] While on the one hand these technologies may produce beneficial effects for diagnosis and treatment of serious diseases, on the other hand they pose several risks in terms of protection of individuals' rights.

This paper will seek to analyse the risks associated with the application of AI technologies in the field of genomic diagnostics in relation to the protection of personal data and to assess whether the current EU legal framework can effectively face them and, if not, which further regulatory interventions would be necessary.

The paper will be structured as follows. Paragraph 1 will introduce AI with specific reference to machine learning, neural networks and deep learning. Then, it will focus on the application of AI in healthcare, specifically in genomic diagnostics, and its connection with big data. Paragraph 2 will analyse the main data protection implications and the risks that AI poses especially in relation to profiling, automated decision-making and opacity. Paragraph 3 will examine the current EU legal framework for the protection of personal data and its adequacy to regulate AI technologies for genomic diagnostics. In particular, the effectiveness of the GDPR to keep up with the recent technological developments will be assessed. Finally, Paragraph 4 will investigate alternative instruments like soft law and medical ethics that may add value to the tools currently in place and straighten the safeguard of individuals' fundamental rights.

1. An overview of artificial intelligence, machine learning and deep learning.

Artificial intelligence (AI) is among the most important and debated drivers of technological development of the last decades and, especially, the last years.[8] Several different definitions of AI have been proposed (one of the most

[5] A De Paor, 'Advancing Genetic Science and New Technologies' in *Genetics, Disability and the Law: Towards an EU Legal Framework* (Cambridge University Press 2017).
[6] D Cirillo, A Valencia, 'Big data analytics for personalized medicine' (n 2).
[7] Nuffield Council on Bioethics, 'Artificial intelligence (AI) in healthcare and research Nuffield Council' [2018].
[8] Modern studies on artificial intelligence date back to the early works of Alan Turing, John McCarthy, Arthur Samuels, Alan Newell, and Frank Rosenblatt, among others. In particular, artificial intelligence was officially born in 1956 during the workshop organised by John McCarthy at the Dartmouth Summer Research Project on Artificial Intelligence with the goal to find how to make machines simulate aspects of human intelligence. In the proposal for that workshop McCarthy used for the first time the term "artificial intelligence" explaining that "the goal of AI is to develop machines that behave as though they were intelligent" (see J

recent is the one suggested by the EU Commission in the Communication on AI)[9] but, despite the lack of a universally accepted definition, the common goal of AI researchers is to create a system that acts in a rational way, namely by choosing the best action to achieve a certain goal.[10] To do so, in simple terms, AI systems through sensors perceive the external environment and collect data from it (*input*). The data coming from the sensors is transformed into information understandable by the system (*knowledge representation*) that reasons on such information (*knowledge reasoning*) to decide what the best action is; finally, it takes the action through actuators (*output*).[11] To perform this function, AI systems rely on algorithms, sequences of unambiguous, well-defined, computer-implementable instructions to execute a task, usually to solve a class of problems or to perform a computation.[12]

The main limit of early AI systems was that a formal representation of the relevant knowledge had to be provided in advance by humans since the system could only deal with known situations but was unable to address new cases out of its knowledge base.[13] A step forward was the development of machine learning (ML),[14] an AI system able to automatically improve its performance at a task by learning from experience and input data, just as humans do.[15]

A particular method of ML is "artificial neural network" (ANN), so called because it simulates the human brain made of neurons which receive and transmit information. Similarly, artificial neural networks are a net of nodes, called "neurons" or "perceptrons", arranged in multiple layers each of which connected to the layers on either side. Neurons in the first layer receive information from the outside (*input units*). The information is processed by neurons in the internal layers (*hidden units*) and the last layer generates the

---

McCarthy, ML Minsky, N Rochester, CE Shannon, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence' [1955]).

[9] "*Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications*)", Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM (2018) 237 (final).

[10] SJ Russell, P Norvig, *Artificial Intelligence: A Modern Approach* (3rd edition, Prentice Hall, 2009).

[11] High-Level Expert Group on Artificial Intelligence, 'A definition of AI: Main capabilities and scientific disciplines' made public on 8 April 2019.

[12] D Harel, YA Feldman, *Algorithmics* (Addison Wesley, 2004).

[13] European Parliamentary Research Service, Scientific Foresight Unit (STOA), 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' June 2020.

[14] Machine Learning has been defined as the "field of study that gives computers the ability to learn without being explicitly programmed". See AL. Samuel, 'Some Studies in Machine Learning Using the Game of Checkers', (1959) 3 IBM J. Res. Dev., 210-229.

[15] There are three main machine learning approaches. (i) Supervised learning: the machine learns through "supervision" or "teaching"; it is provided with a "training set", that is a set of labelled data, and is instructed on how this data has to be categorised. The learning algorithm (trainer) uses this set to learn how to identify specific features, infers the logic underlying the set and builds a model. Then, the model is applied to new data in order to identify and categorise unseen data based on patterns detected in the training set. (ii) Unsupervised learning: the system does not receive external instructions in the form of labelled data but finds patterns on its own. (iii) Reinforcement learning: the system learns by trial-and-error through a "reward and punishment" approach. It is not provided with training data but learns by the outcome of its own actions: if it is given a reward signal, the algorithm (learner) learns that the action is right, if no reward follows the action, this is learnt to be wrong. For a more in-depth analysis see P Natarajan, B Rogers, 'Applied Machine Learning for Healthcare" in P Natarajan, JC Frenzel and DH Smaltz (eds.), *Demystifying Big Data and Machine Learning for Healthcare* (CRC Press 2017), 29.

result (*output unit*). The connection between one layer and another is associated with a number called "weight", which defines the value of each input feature in predicting the final output (i.e. how important a certain genetic variation is in developing a disease). When the neural network is trained on the training set, it is initialised with a set of weights. During the training phase weights are adjusted based on whether the outputs are right or wrong. If the output matches the labelled data, the weight is kept. If the output is sub-optimal (i.e. doesn't match the label), the learning algorithm adjusts the weight until the network, when presented with that input, will generate the correct output.[16]

Neural networks may be more or less complex depending on the number of hidden layers they have. A subset of neural networks is "deep learning" which includes several hidden layers, and each layer learns from the layer below: it receives as data input the previous layer's output, so the deeper the layers, the more complex the features that nodes can recognise.[17] As a consequence, the network is more accurate and with less need of human guidance.

1.1 Application of AI in genomic diagnostics.

AI, in particular machine learning and deep learning, may be extensively deployed in genomic diagnostics to detect disease at an earlier stage thus improving patients' quality of life. Such technologies are not intended to replace physicians but rather to augment their capabilities and make more efficient and cost-effective routine standardised tasks.[18] Different algorithms can perform different tasks, but the main areas where AI has proven helpful are classification, image and video recognition, clustering, and prediction.[19] Often these functions are combined to achieve more effective results. In particular, image recognition is used to train neural networks to predict disease, especially in oncology.[20]

Important results in the use of AI in genomic diagnostics have already been achieved and further are expected by the next years.[21] An example is IDx-DR, a

[16] European Parliamentary Research Service, Scientific Foresight Unit (STOA), 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' June 2020.
[17] J Schmidhuber, 'Deep Learning in Neural Networks: An Overview' (2015) 61 Neural Networks.
[18] See for instance KY Ngiam, IW Khor, 'Big Data and Machine Learning Algorithms for Health-Care Delivery' (2019) 20 The Lancet Oncology.
[19] Classification is carried out by deep learning algorithms that are trained with a sheer number of examples to analyse symptoms and classify them into labelled diseases in order to suggest possible diagnosis or identify patients with high readmission risk. Image and video recognition means that deep learning systems can detect objects in complex images, label and classify them into disease types. Clustering is the function of AI systems that identify similarities and connections among items and group them accordingly; typically, the algorithm is given a set of features for each item and a number of clusters to create, and it will combine such features and divide the items into the given number of clusters). Prediction is achieved by neural networks able to analyse large amounts of data as input, combine them and produce as output the likelihood that a patient will get a certain disease in the next future.
[20] The network is provided with raw image data used as training data to identify highly predictive features (regions of interest). Such regions of interest are combined with other relevant data – in particular, genomic data – to build a model to detect patterns in new data. This is the so-called genomic survival convolutional neural network (GSCNN model). See P Mobadersany *et al.*, 'Predicting Cancer Outcomes from Histology and Genomics Using Convolutional Networks' (2018) 115 Proceedings of the National Academy of Sciences.
[21] For instance, Google is collaborating with health delivery networks to build prediction models from big data to warn clinicians of high-risk conditions, such as sepsis and heart failure, and provide them decision support to find the best diagnosis and treatment for patients. Other firms, such as Foundation Medicine

software program that uses a ML algorithm to analyse the retinal images from patients, producing one of two possible screening results: positive (more than mild diabetic retinopathy) or negative (mild diabetic retinopathy or lower).[22]

AI has also been used in the fight against amyotrophic lateral sclerosis (ALS), a devastating neurodegenerative disease caused by mutations of RNA-binding proteins (RBPs). [23] The number of RBPs currently associated with ALS represents only a small fraction of the total RBPs present in the human genome and it has been hypothesised that further unidentified RBPs may be linked to ALS. On this basis, IBM Watson has been developed to predict new potential RBPs in ALS.[24]

IBM also developed other AI systems to support physicians in making treatment decisions for different types of cancer [25]. One is Watson for Oncology (WFO), a system trained with different data sources like biomarkers derived from the patients (e.g. sex, age, type of tumour), medical literature, national treatment standards and medical records. Based on the analysis of such data, the algorithm suggests what treatment options are available and ranks them in three categories (recommended, for consideration, and not recommended) according to their suitability for the patient.[26] Several studies have been conducted to examine the concordance between the treatment recommendation proposed by WFO and actual clinical decisions by expert oncologists.[27]

A further development is IBM Watson for Genomics (WfG), an AI system for treating cancer with a personalised approach. To date, the analysis of patient genomes is performed manually by teams of human experts and may take weeks. WfG aims at supporting oncologists by analysing large volumes of genomic data.[28] WfG is first trained with databases of genomic alterations,

---

and Flatiron Health, both owned by Roche, specifically focus on diagnosis and treatment recommendations for certain cancers based on their genetic profiles given the difficulty of human clinicians to understand all genetic variants of cancer and their response to new drugs and protocols. See T Davenport, R Kalakota, 'The potential for artificial intelligence in healthcare' (2019) 6 Future Healthcare Journal, 94-98.

[22] See MD Abràmoff *et al.*, 'Pivotal Trial of an Autonomous AI-Based Diagnostic System for Detection of Diabetic Retinopathy in Primary Care Offices' (2018) 1 npj Digital Medicine.

[23] RNA-binding proteins (RBPs) are proteins having important functions in the regulation of gene expression. See C Oliveira et al., 'RNA-binding proteins and their role in the regulation of gene expression in *Trypanosoma cruzi* and *Saccharomyces cerevisiae*' (2017) 40(1) Genetics and Molecular Biology, 22-30.

[24] To achieve this goal the system has first been trained with published literature from which the system extracted specific features to identify new connections between genes, proteins, drugs, and diseases. As a result, Watson created a model of the known set of RBPs linked to ALS in such a way to apply that model to an unseen set of other RBPs, in order to rank all the new RBPs by similarity to the known set. Finally, the top-ten-ranked RBPs are validated by medical experts. For more details see N Bakkar *et al.*, 'Artificial Intelligence in Neurodegenerative Disease Research: Use of IBM Watson to Identify Additional RNA-Binding Proteins Altered in Amyotrophic Lateral Sclerosis' (2017) 135 Acta Neuropathologica.

[25] At present these systems, now in use in some hospitals especially in Asia, still have some limitations with the risk of producing inaccurate predictions or proposing incorrect treatment recommendations. However, they demonstrate that technology and medicine are moving towards this direction and in the next future we could likely assist to relevant developments in this sense. See C Ross, I Swetlitz, 'IBM's Watson supercomputer recommended "unsafe and incorrect" cancer treatments, internal documents show' (2018) STAT.

[26] A Tupasela, E Di Nucci, 'Concordance as Evidence in the Watson for Oncology Decision-Support System' (2020) AI & Society.

[27] Among others N Zhou *et al.*, 'Concordance Study between IBM Watson for Oncology and Clinical Practice for Patients with Cancer in China' (2018) 24 The Oncologist.

[28] K Rhrissorrakrai, T Koyama, L Parida, 'Watson for Genomics: Moving Personalized Medicine Forward' (2016) 2 Trends in Cancer.

published literature and clinical studies; then, it receives as input data the patient's cancer genetic variants and evaluates each variant using advanced cognitive analytics, an analytical technique that analyses large datasets by using AI.[29] As an output, it presents a report of relevant therapies along with links to the relevant medical literature. Doctors will then review the report together with additional clinical evidence to make an informed treatment decision.[30]

1.2 Big Health Data and AI.

To efficiently operate ML systems need to process large amounts of data. The more numerous and diverse the data they are trained on, the more accurate and correct the outputs, especially when AI systems are used to make diagnosis predictions or suggest treatment recommendations. [31] However, having more data also gives rise to more problems, as it will be extensively illustrated in the following paragraphs.

In the past, collecting and analysing data was time-consuming and expensive; thus, physicians only collected strictly necessary data. Not surprisingly AI has reached a turning point over the last years, when the amount of data gathered and processed around the world has exponentially grown and data analysis has become much cheaper and faster.[32]

Today data collection has evolved under two aspects: (i) the number of data available is much higher; and (ii) the content of such data is much broader and diverse. This phenomenon is commonly referred to as "big data".[33] Big data has revolutionised healthcare: while in the past health-related data only included data collected in the healthcare environment by health actors, with the advent of big data this category has included any types of data from which it is possible to infer information about health (data related to physical, environmental, or biological aspects, as well as social, economic, or individual *status*, lifestyle, commercial preferences, so-called "big health data"). Furthermore, data may be collected from an array of (non-medical) sources like social networks that aggregate information about people's preferences, interests, contacts, etc.;[34] smartphones, able to track people's movements, activities and social interactions; "mHealth apps" developed to store health-related data and keep

[29] See 'Cognitive Analytics — Combining Artificial Intelligence (AI) and Data Analytics', Ulster University, Cognitive Analytics Research Lab at https://www.ulster.ac.uk/cognitive-analytics-research/cognitive-analytics.

[30] K Itahashi *et al.*, 'Evaluating Clinical Genome Sequence Analysis by Watson for Genomics' (2018) 5 Frontiers in medicine.

[31] WN Price, IG Cohen, 'Privacy in the Age of Medical Big Data' (2019) 25 Nature Medicine.

[32] It is estimated that between 1987 and 2007 alone the amount of data in the world grew one hundred times. See M Hilbert, P Lopez, 'The World's Technological Capacity to Store, Communicate, and Compute Information' (2011) 332 Science.

[33] No unanimous definition of big data exists, but according to a generally accepted opinion, it may be described by the "three Vs": volume (large amounts of data), velocity (high speed of access and analysis), and variety (substantial data heterogeneity across individuals and data types). See Executive Office of the President. Big data: seizing opportunities, preserving values https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf (2014).

[34] S Hoffman, 'Big Data's New Discrimination Threats Amending the Americans with Disabilities Act to Cover Discrimination Based on Data-Driven Predictions of Future Disease' in G Cohen, A Hoffman and W Sage (eds.), *Big Data, Health Law, and Bioethics* (Cambridge University Press, 2017).

track of users' health and physical conditions; and Internet of Things (IoT) devices that, through their sensors, perceive external inputs, process them and interact with each other.[35]

Such an amount of data requires adequate data analysis methods to process it, and these are AI technologies, in particular ML that is able to continuously learn from training data and apply the learnt model to new and unseen data. It follows that algorithms trained on big health data not only may confirm existing hypothesis and support existing diagnosis but can also suggest new hypothesis and make predictions before symptoms are being experienced by the patient.[36]

Such predictions are mainly based on correlation as opposed to causation that, on the contrary, has always been the basis for scientific research. Traditionally, indeed, any scientific position could only be claimed by understanding causes, thus after having found and proved linkages between causes and effects. By contrast, the typical big data approach is correlation, meaning that algorithms produce outcomes based on statistical analysis. Hence, not necessarily a cause-effect relation is demonstrated, but rather data are associated according to patterns identified in the training set in such a way to predict the occurrence of health-related events.[37] Correlation is particularly significant in genomics where identification of the causative relation between genetic mutations and disease has long been limited. Correlation has several benefits against causation: it is quick, automatic, and inexpensive, as opposed to costly and time-consuming causation approaches. Furthermore, links between variants and factors are more likely to emerge, also considering that it is not uncommon that associations are clearly experienced but difficult to prove in theory. Yet, there are some side-effects. The main problem is demonstrating to what extent a genetic mutation impacts on the risk to develop a particular disease.[38] In addition, without a theory to understand the prediction, the outcome achieved cannot be generalised and can only be used in the specific context. Finally, in the absence of a solid basis the risk of error and inaccuracy is much higher.[39]

2. The implications of AI on data protection.

As it emerges from the previous paragraph, the key to have efficient AI systems is training algorithms with huge amounts of personal data.[40] Given that, it is not surprising that several issues arise when AI is deployed in genomic

[35] An example are "wearables", tools that collect relevant health data such as blood pressure, glucose, sleep apnea, cardiac and other monitors and interact with smartphones or directly with third parties (e.g. GPs). Several other IoT devices surround people, able to collect enormous amounts of data of any kind (for instance domotic assistants know habits, preferences and behaviours of the residents of the house).
[36] V Mayer-Schönberger, E Ingelsson, 'Big Data and Medicine - a Big Deal?' (2018) 283 Journal of Internal Medicine.
[37] TZ Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall Law Review.
[38] MKK Leung *et al.*, 'Machine Learning in Genomic Medicine: A Review of Computational Problems and Data Sets' (2016) 104(1) Proceedings of the IEEE, 176-197.
[39] *Ibid.*
[40] Under Art. 4 (1)(1) GDPR personal data are defined as "namely data related to an identified or identifiable subject".

diagnostics. Such issues relate both to the collection of personal data as input and to the processing of data resulting in output.

As for the collection, data not directly related to health (obtained from different sources) are also necessary to properly train algorithms. Herein, people providing their personal data may not know how and for what purposes such data will be used because at the time of data collection it may be difficult to exactly foresee the future uses of data.[41] Besides, data can be cross-context, meaning that they can be used for multiple different purposes, also in different fields and by different data controllers.[42] Hence, data subjects might not be adequately informed and, thus, cannot maintain an effective control over their data.

Another aspect concerns the quality of input data: if data is incorrect or altered, the outcome will be inaccurate. Input data may be altered not only when it is false or wrong, but also when it is biased. If datasets reflect existing biases against minorities or other vulnerable groups (e.g. entrenched overdiagnosis of schizophrenia in African Americans),[43] such biases will be reproduced in the outcomes.[44] Biases may also be unintentional, because they are always latent in society, reflecting cultural or organisational values.[45] Therefore, even if clear sensitive data like race, age or gender were excluded, other apparently neutral data (e.g. postal code) could be associated in such a way to result in biased outcomes.[46] In addition, biases can result from non-representation of marginalised groups: datasets used to train algorithms might not adequately represent the whole population because there are not enough data related to certain vulnerable groups like racial minorities, immigrants, or people with low socioeconomic *status*.[47] One of the reasons is that such groups have no access to the most common data sources like social media, smartphones, wearables and often even the Internet and healthcare itself, thus not being represented in clinical data.[48] Another reason is the absence of studies on certain segments of the population. Genomic diagnostics, in particular, has a history of under-representation of ethnically diverse populations since genetic studies of human disease have always been predominantly based on populations of European ancestry.[49] These exclusions

[41] IG Cohen *et al.*, 'Introduction' in G Cohen, A Hoffman and W Sage (eds.), *Big Data, Health Law, and Bioethics* (Cambridge University Press, 2017).
[42] WN Price, IG Cohen, 'Privacy in the Age of Medical Big Data' (n 31).
[43] HW Neighbors *et al.*, 'The Influence of Racial Factors on Psychiatric Diagnosis: A Review and Suggestions for Research' (1989) 25 Community Ment Health J, 301–11.
[44] D Schönberger, 'Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications' (2019) 27 International Journal of Law and Information Technology, 171–203.
[45] M Hardt, 'How Big Data is Unfair', 26 September 2014, <https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de>.
[46] A Romei, S Ruggieri, 'A Multidisciplinary Survey on Discrimination Analysis' (2014) 29 The Knowledge Engineering Review, 582.
[47] D Schönberger, 'Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications' (n 44).
[48] SE Malanga *et al.*, 'Who's Left Out of Big Data? How Big Data Collection, Analysis, and Use Neglect Populations Most in Need of Medical and Public Health Research and Interventions' in G Cohen, A Hoffman and W Sage (eds.), *Big Data, Health Law, and Bioethics* (Cambridge University Press, 2017).
[49] Recent studies indicate that the proportion of individuals included in GWAS who are not of European descent is less than 20%. In particular, individuals of African and Latin American ancestry, Hispanic people and native or indigenous peoples represent together less than 4%. See AB Popejoy, SM Fullerton, 'Genomics

reflect pre-existing health disparities and amplify them, thus bearing the risk of causing serious diagnosis mistakes.[50]

When it comes to the generation of outcomes one of the main issues is the "opacity" of AI systems (more precisely, of algorithms).[51] Given that it combines large-scale high-quality datasets with sophisticated predictive algorithms and use implicit, complex connections between multiple variables, ML may identify patterns and make associations within such a high number of variables and with such an elaborate computation that it is extremely hard for the human mind to grasp the underlying logic. As a consequence, neither doctors nor AI experts would be able to fully understand how the data is processed and how the output is obtained.

Because of this opacity AI systems have been defined as "black boxes".[52] The use of black boxes in genomic diagnostics may lead to enormous benefits. Indeed, genomic datasets are so vast and the relationships among them and with other variables are so complex that they are not fully understood in medical literature yet. Hence, associations made by algorithms, although opaque, may suggest new treatment options and make more specific predictions.[53] On the other hand, black boxes could negatively affect the patients' right to be informed on how their data is processed and how decisions concerning themselves are taken.[54]

As such, the opacity of algorithms limits individuals' autonomy of identity, namely the ability of individuals to build their own identity without external influences. The reason is that based on the machine outcome patients are classified and grouped into clusters (e.g. based on the presence of a tumour, the likelihood of success of a treatment, the prediction of risk and survival) and subsequent decisions will be taken in relation to the cluster as a group, regardless of the identity of the group members as individuals. Yet, groups do not perfectly reflect individuals because they represent only some aspects of their identity.[55] It follows that decisions might be taken for all the members of the group, based on their common features, without taking into account the differences existing among them and the further characteristics that each member has and that contribute to delineate their identity. In the field of genomic diagnostics the consequences may be particularly dangerous because, for instance, all patients with the same type of cancer could be medically treated in the same way without considering that the treatment could have different consequences depending on their lifestyle or the existence of further genetic variants.

---

is failing on diversity' (2016) 538 Nature, 161–164; G Sirugo, SM Williams, SA Tishkoff, 'The Missing Diversity in Human Genetic Studies' (2019) 177(1) Cell., 26-31.

[50] An example is a study conducted to detect skin cancer by using ML, where fewer than 5 per cent of the images the model was trained on were from individuals with dark skin. See J Zou, L Schiebinger, 'AI can be Sexist and Racist — it's time to make it Fair' (2018) 559 Nature, 324–6.

[51] WN Price II, 'Black-Box Medicine' (2014) 28 Harvard Journal of Law & Technology, 419.

[52] One of the first authors to propose the idea of black boxes was Frank Pasquale in 2015. See F Pasquale, *The black box society: The secret algorithms that control money and information* (Harvard University Press 2015). See also WN Price II, 'Black-Box Medicine' (n 51).

[53] WN Price II, 'Black-Box Medicine' (n 51).

[54] BD Mittelstadt, P Allo *et al.*, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 Big Data & Society.

[55] B Mittelstadt, 'From Individual to Group Privacy in Biomedical Big' in G Cohen, A Hoffman and W Sage (eds.), *Big Data, Health Law, and Bioethics* (Cambridge University Press, 2017).

Finally, ML outcomes could lead to discriminatory treatments of data subjects. In particular, within the healthcare environment medical predictions and diagnosis could lead to discriminatory treatment plans if relied on biased data. In addition, should third parties (e.g. employers, health insurances, financial services providers) access them, they could take advantage of such outcomes to discriminate vulnerable data subjects.[56] Besides, the opacity of algorithms makes it hard to prove that discrimination has actually occurred.[57]

3. Application of European Data Protection Law to AI.

This paragraph will examine the European General Data Protection Regulation (GDPR) [58] to assess how it deals with the data protection issues raised by the use of AI in genomic diagnostics and evaluate whether it is sufficient to ensure adequate protection of patients' personal data. In particular, three aspects will be taken into consideration: the GDPR underlying concepts, its fundamental principles and the data subjects' rights.

3.1 The GDPR underlying concepts.

First of all, the material scope of the GDPR covers "personal data", defined as "*any information relating to an identified or identifiable natural person*".[59] This notion is based on the concept of identifiability, so that anonymous data fall outside the scope of the Regulation. This choice was justified when processing focused on individuals, but it seems no longer meaningful in a world dominated by big data and algorithms that process large amounts of data not related to any specific person. [60] In particular, the deployment of ML in genomic diagnostics requires the collection of huge datasets to train the algorithm and make it as much accurate as possible, but it is not necessary that such data is linked to identified data subjects since – in the training phase – it is only their aggregation that matters. Therefore, data may be anonymised to easily avoid the GDPR obligations with the consequence that no protection will be ensured to people whose data is collected and used to identify patterns and create clusters. In this perspective identifiability represents a limit to data protection since under the GDPR an effective protection is ensured only when data can be linked to a precise person. However, as noted before, AI systems are able to make inferences from input data based on statistical associations, so the mere fact that a person is included in a group allows to collect a lot of data about him/her because, even though his/her name would not be known, the group characteristics would describe that person with sufficient accuracy. As a

[56] S Hoffman, 'Big Data's New Discrimination Threats Amending the Americans with Disabilities Act to Cover Discrimination Based on Data-Driven Predictions of Future Disease' (n 34).
[57] WN Price, IG Cohen, 'Privacy in the Age of Medical Big Data' (n 31).
[58] Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive 95/46/EC, 2016 O.J. L 119/1.
[59] Art. 4(1) GDPR.
[60] EG González, P de Hert, 'Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles' (2019) 19 ERA Forum, 597–621.

consequence, it should not be necessary to identify a person with absolute certainty to provide for data protection; rather, it should be enough to know that a person is included in a certain group.[61]

A second aspect, strictly related to the previous one, is the individual dimension: the GDPR regulates data protection as an individual right and focuses on individuals' protection. However, data processing in genomic diagnostics mainly concerns group data: algorithms manage to discover unknown patterns among individuals with certain characteristics thus creating groups based, for instance, on the likelihood to develop a disease or the chance to survive. In this case, risks do not concern directly members of the group as such, but rather the group itself. [62] Indeed, by processing group data, controllers are able to create "inferences", namely non-verifiable information, opinions, or assessments[63] that will be used to take decisions towards any patients included in that group. Patients have no rights on such inferences, given that the GDPR focuses primarily on mechanisms related to the input side (collection and processing), while mechanisms addressing outputs (i.e. inferred data, profiles, decisions) like, for example, the right to explanation, are far weaker (as it will be better explained below). Yet, outputs are the ones that pose major risks, given that problems do not lie much with data collection, but rather with what can be inferred from such data and the decisions that can be taken based on this knowledge (e.g. the decision to apply a therapeutic plan or make surgery based on the likelihood to develop a disease). [64]

Another cornerstone of the GDPR is the distinction between sensitive and non-sensitive data. [65] The *ratio* of this distinction is ensuring stronger protection for sensitive data by introducing further limitations for processing and providing data subjects with major safeguards. However, such a distinction is challenged by AI and big data analytics because algorithms can infer sensitive data even from non-sensitive data, thus shifting from one category to another. In particular, a lot of non-medical data collected from different sources can be used to create medical profiles and make inferences about health. This fluidity makes the abovementioned distinction fundamentally flawed and almost useless because any data could potentially become sensitive if used to infer information about health.[66] For this reason, it may become difficult to set the point when non-sensitive data should start being treated (and protected) as

[61] On the distinction between identifiable and non-identifiable data in the Big Data era see CJ Bennett, RM Bayley, 'Privacy Protection in the Era of "Big Data": Regulatory Challenges and Social Assessments', in B van der Sloot, D Broeders and E Schrijvers (eds.), *Exploring the Boundaries of Big Data* (WRR/Amsterdam University Press, 2016), 205.

[62] EG González, P de Hert, 'Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles' (n 60).

[63] Article 29 Data Prot. Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP136, at 8 (June 20, 2007).

[64] S Wachter, B Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 1 Columbia Business Law Review.

[65] "Sensitive data" are so called because they relate to the inner – and more sensitive – sphere of individuals (e.g. health, religion, sexual orientation) and thus unlawful processing would produce particularly serious consequences on data subjects. The terminology "sensitive data" was used under the Data Protection Directive. Art. 9 GDPR defines such data as "*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*".

[66] TZ Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (n 37).

sensitive data.

Finally, the GDPR is based on the idea that personal data can be processed provided that data subjects maintain control over data related to them. In this perspective the GDPR grants individuals several rights (e.g. right of access, right to rectify, erasure, object) and includes among the lawful basis for processing data subjects' consent [67] that must be freely given, specific, informed, and unambiguous.[68] This is referred to as the "notice-and-consent" model according to which patients must be adequately informed about the processing of their personal data in order to take meaningful decisions about it. Yet, this model has been weakened by AI-based technologies that make the explanation and understanding of data processing much more complicated especially to non-expert data subjects. Herein, even though the GDPR imposes on controllers to provide data subjects with all the relevant information about the processing, patients could hardly understand it and make fully conscious choices. Hence, behind the façade of self-determination data subjects risk not to be actually protected. This should lead regulators to reconsider the role of data subjects in the processing of personal data, at least when the processing is extremely complex as the AI-based processing for diagnostic purposes.[69] Rather than placing on patients the burden to understand how the processing is carried out and what are the best decisions to protect their rights, a stronger obligation should be imposed on data controllers to take all the measures necessary to protect individuals even out of their control. Indeed, it would require a huge effort to patients to fully understand what is behind data processing and not all of them might have time, resources, and capability to understand it. On the contrary, developers and medical structures deploying AI systems are in a better position to assess and guarantee that the processing is safe.[70] This approach is not new but is already adopted in other regulatory fields involving information too complex to be understood without expert knowledge like, for instance, food industry, building engineering and car safety.[71] It would mean a shift from individual consent to *ex ante* assessments (carried out by controllers and external independent expert entities) aimed to certify the security of the processing and the absence of potential risks and harms for individuals.

3.2 The GDPR fundamental principles.

Art. 5 GDPR sets the fundamental principles to be respected when processing personal data. In particular, Art. 5(1)(a) sets the principles of lawfulness, fairness and transparency, meaning that the processing must have

[67] Art. 6(1)(a) GDPR.
[68] Art. 4(11) GDPR.
[69] A Mantelero, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33 Computer Law & Security Review, 584–602.
[70] Developers – being the ones who design the system – can more easily understand how it works and guarantee its safety and have the competences and the resources to certify, even with external bodies, that the system respects safety standards. At the same time medical structures have a direct relationship with the developer to understand the system functioning and have the technical resources to test the safety of the system before putting it into use.
[71] V Mayer-Schönberger, E Ingelsson, 'Big Data and Medicine - a Big Deal?' (n 36).

a lawful basis[72] and must be carried out in a fair and transparent manner. Transparency is extremely important because it allows data subjects to know how their data is processed and maintain control over it, thus it is strictly linked to the right to be informed and the right of access (that will be analysed in-depth in the next paragraph). Yet, transparency is threatened by the opacity of algorithms that makes it difficult to explain on what basis data is aggregated, how clusters are created, and how outputs are generated.

Art. 5(1)(b) sets forth the principle of "purpose limitation"[73] whose *ratio* is to prevent data controllers from using data for other purposes than those for which it was initially collected. Yet, such a principle may hinder the development of AI for genomic diagnostics since ML algorithms – to make precise inferences and generate accurate outputs – must be trained on large volumes of data that could be collected from several sources even not directly related to health (e.g. social networks, IoTs, etc.). When this is the case, data is initially collected for purposes different from training algorithms for genomic diagnostics and, at the moment it is collected, neither the controller nor the data subject might specifically know that it could also be used for diagnostic purposes. Thus, a strict application of the purpose limitation principle, albeit meant to protect data subjects, could end up posing a limit to training algorithms.[74]

Other principles are "data minimisation"[75] and "storage limitation"[76] that require respectively to collect only data adequate, relevant and necessary to achieve the purposes for which it is processed and keep data for no longer than necessary to achieve these purposes. These principles aim to prevent data controllers from collecting and retaining data not necessary for the processing, thus exploiting data for further unspecified purposes. On the other hand, such a limitation may curtail the deployment of AI systems for genomic diagnostics because, as already mentioned, algorithms must be trained on large amounts of data to identify relevant patterns and generate reliable outputs. Yet, data that could potentially be used to train algorithms but are not or no longer necessary to achieve the initial purpose (i.e. the purpose for which it is processed in the first place) cannot be collected. This could reduce the amount

[72] Among those listed in Articles 6 and 9 GDPR.
[73] According to such a principle personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". See Art. 5(1)(b) GDPR.
[74] A Mantelero, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (n 69). Art. 5 partly derogates this principle when further processing is not incompatible with the original purposes. Nevertheless, doubts remain on when processing may be considered "compatible". On this regard, Art. 5(1)(b) specifies that processing for "statistical purposes" is not incompatible, but according to Recital 162 statistical purposes imply that the result or processing "are not used in support of measures or decisions regarding any particular natural person". This cannot be the case for data used to train algorithms for diagnostic purposes, given that the results will likely ground medical decisions concerning patients. Indeed, training data are analysed by the algorithm to build the model that will be applied to new cases to suggest medical decisions (e.g. therapeutic plans). This means that, based on the inferences and the correlations found in the training datasets, the algorithm identifies the best medical decisions related to each patient's personal circumstances. Secondly, Art. 6(4) lists the criteria to be taken into account to assess the compatibility of further processing and mentions, inter alia, the link with the original purpose, the context in which data have been collected, and the nature of data. Under these terms, collection of personal data based for instance on the preferences expressed by the user on a social network could hardly be linked with the purpose of training algorithms to diagnose diseases.
[75] Art. 5(1)(c) GDPR.
[76] Art. 5(1)(e) GDPR.

of data available to train algorithms thus undermining their effectiveness.[77]

3.3 The GDPR data subjects' rights.

Chapter III of the GDPR grants data subjects a series of rights related to the processing of their personal data.[78]

Arts. 13 and 14 impose on the controller to provide data subjects with relevant information about the processing.[79] Such information has to be provided either at the time of data collection (Art. 13) or at the first communication with the data subject (Art. 14), thus only covering *ex ante* explanation about system functionality. Besides, the expression "*envisaged consequences of such processing*" refers to future consequences not occurred yet,[80] while no information on the reasons and the effects of specific decisions can be released, since these require that a decision has already been taken.[81]

Similarly, Art. 15 confers on data subjects the right to access information about the processing. Although in this case the right can be exercised in any moment, without the time limit set in Arts. 13-14, reference remains to the "*envisaged consequences*", meaning that the relevant information is supposed to be provided before a decision has occurred. As in the previous case the right only ensures *ex ante* explanation about the functioning of the automated decision system, but no *ex post* explanation about the grounds and the implications of a specific decision is required.[82]

A fundamental right for AI-based diagnostic data processing is set forth in Art. 22(1), whose scope is widely debated in literature. It establishes as a general rule the right of data subjects not to be subject to decisions based solely on automated processing including profiling.[83] Actually, as the Article 29 Working Party clarified, such a provision should be interpreted as a prohibition to data controllers rather than a right, with the consequence that controllers must refrain from automated decision-making without data subjects having to actively require it.[84] Art. 22(2) admits some exceptions to this general rule, allowing automated decision-making under certain conditions,[85] but even when these conditions are fulfilled, special categories of personal data can be used for automated decision-making only with data subjects' consent (or for

[77] TZ Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (n 37).
[78] These are the right to be informed (Arts. 13-14), right of access (Art. 15), right to rectification (Art. 16), erasure (Art. 17), restriction of processing (Art. 18), data portability (Art. 20), right to object (Art. 21), and right not to be subject to automated decision-making (Art. 22).
[79] In particular, information shall be provided about "*the existence of automated decision-making, including profiling, […] and, […], meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*".
[80] EG González, P de Hert, 'Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles' (n 60).
[81] S Wachter *et al.*, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) International Data Privacy Law.
[82] *Ibid.*
[83] Art. 22(1) says "*The data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*".
[84] Article 29 Working Party (A29WP), 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251, 3 October 2017).
[85] In particular, when it is necessary for performing a contract between the data subject and the data controller or when it is based on the data subject's consent.

reasons of substantial public interest).[86] Furthermore, when the abovementioned exceptions apply, the controller has to inform the data subject and adopt adequate safeguards, in particular ensure the right "*to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*",[87] the so-called "human in the loop".[88] Instead, no explanation of how the processing is carried out or how the results are achieved is imposed, so that some scholars, in particular Wachter et al., have argued that "the GDPR does not […], implement a right to explanation, but rather [a] right to be informed".[89] Such a conclusion has been rebutted by Selbst and Powles who suggest that Art. 22, although does not directly set forth a right to explanation, supports the existence of that right which is derived from Articles 13-15, in particular in the part where they acknowledge data subjects' right to "*meaningful information about the logic involved*" in automated decisions.[90]

In any case, the right of explanation should not be regarded as a panacea for all the problems posed by algorithms.[91] Indeed, the way in which algorithms work is not always interpretable: the "black box" model makes it difficult to understand the correlations between input data made by algorithms to find patterns and create clusters. Therefore, the "logic" behind automated systems might not be fully explainable to humans and simplifying such systems in order to make them human interpretable could result in reducing their predictive performance.[92] Secondly, even when experts would manage to interpret the systems, these could be hardly explicable to non-expert data subjects (e.g. patients). The result would be a "transparency fallacy",[93] that is, an illusion to provide data subjects with enough information to allow them to maintain full control over their personal data, while, in fact, such information is not meaningful if cannot be really understood.[94]

---

[86] Art. 22(4) GDPR.
[87] Art. 22(3) GDPR.
[88] L Edwards, M Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review, 18.
[89] S Wachter *et al.*, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (n 81).
[90] AD Selbst, J Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 Int'l Data Privacy L., 233.
[91] B Casey *et al.*, 'Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34 Berkeley Tech LJ, 143.
[92] L Edwards, M Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For' (n 88).
[93] This notion has been first introduced in relation to consent, as giving data subjects the illusion to take control of the use of their personal data. See DA Heald, 'Varieties of Transparency' in C Hood and D Heald (eds.) *Transparency: The Key to Better Governance?: Proceedings of the British Academy* (Oxford University Press, 2006), 135 .
[94] Apart from the right to explanation, the scope of Art. 22 is narrowed under two aspects. Firstly, para. 1 only applies to decisions based "*solely*" on automated processing, thus implying that as long as there is a human intervention the right should be excluded. Current automated systems are mostly used to support rather than replace human activity, so that just a few of them are entirely autonomous and this would strongly reduce Art. 22 practical relevance. The A29WP clarified that, to be regarded as human involvement, "*any oversight of the decision [should be] meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision*". Doubts still remain concerning the degree of human intervention required to exclude the application of Art. 22(1). In particular, in the field of genomic diagnostics physicians still maintain a certain discretion in deciding whether or not to follow the machine's advice (there is usually a team of medical experts who interpret and discuss the outcome). It may be questioned whether such intervention is sufficient to exclude patients' right not to be subject to

4. Alternative regulatory instruments to deal with data protection issues in AI-based genomic diagnostics.

As emerged in the previous section data protection law is not sufficient to deal with the data protection issues posed by AI. There are in particular two reasons for this. Firstly, there are some misalignments between the GDPR and the development of AI. In particular, the GDPR is still focused on individual protection and grants no rights to groups, while algorithms create clusters where patients are grouped based on aggregated personal data. In addition, the GDPR is based on data subjects' self-determinism (the "notice-and-consent" model) that seems incompatible with the complexity and the opacity of ML. Secondly, data protection law only covers part of the issues posed by AI. Yet, AI-based data processing for diagnostic purposes gives rise to further issues (like discrimination and protection of aggregated data) that are not specifically addressed. Therefore, data protection law needs to be included in a broader framework and combined with other regulatory instruments to ensure adequate protection of patients/data subjects' rights and, at the same time, allow them to benefit of the advantages of AI. [95]

4.1 Medical law.

A first instrument may be medical law that, although not directly addressing AI, includes some provisions which may affect the deployment of AI-based technologies in genetic diagnostics. [96]

The need to respect the privacy of patients and the confidentiality of the

automated decision-making. Secondly, Art. 22(1) only applies when the decision produces legal effects or "*similarly significantly*" affects the data subject. This last expression has been clarified by the A29WP (see A29WP note 84). According to this interpretation automated decisions in the field of genomic diagnostics may be considered as significantly affecting patients and, as such, falling under the scope of Art. 22 given that the exclusion or confirmation of disease as well as the decision to have the patient undergone surgery or the choice of a therapeutic plan affects patients' whole life and all their consequent choices and behaviour.

[95] A piece of this framework is non-discrimination law, given that discriminatory effects are among the main risks posed by AI, especially in the field of genomics, given its history of underrepresentation of some ethnical groups. Non-discrimination has always been one of the fundamental values of the EU, thus it is included in the EU treaties (Art. 2 TEU, Art. 10 TFUE, Art. 21 EU Charter of Fundamental Rights), Member States' constitutions and several EU directives (Directive 2000/43/EC, Directive 2000/78/EC, Directive 2004/113/EC, Directive 2006/54/EC). Yet, non-discrimination law is not always able to deal with the discriminatory effects of AI given that it mainly addresses direct discrimination that, being based on belonging to protected classes (e.g. because of race or gender), is easier to detect and prohibit. However, the most common form of discrimination in AI is indirect discrimination, based on apparently neutral elements (e.g. postal code, pet ownership) that hide protected classes, thus making it difficult to ascertain the existence of discrimination. In the case of indirect discrimination the algorithm is a neutral criterion since it is not discriminatory *per se* but its application may lead to discriminatory results. As a consequence, it falls on data subjects the burden to prove that the decision is discriminatory and lacks an objective justification. In addition, current non-discrimination law mostly addresses traditional protected classes (e.g. based on ethnicity, gender), while discrimination grounded on different elements that do not seem *prima facie* discriminatory (e.g. genetic variants) could fall outside its scope. See P Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law' (2018) 55 Common Market Law Review, 1143-1186; see also FJ Zuiderveen Borgesius, 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' (2020) The International Journal of Human Rights.

[96] The term "medical law" will be used in the following paragraph as generally referring to the branch of law regulating, in particular, the performing of medical operations, the relations between medical operators and patients, medical devices, the prerogatives of medical professionals and the rights of patients.

information they disclose to their physicians has been a cornerstone of medical practice since the Hippocratic oath.[97] More recent is the notion of "informed consent" grounded on respect for human dignity, according to which subjects involved in medical research must be adequately informed of the aims, methods, benefits, potential risks and any other relevant aspects of the treatment, as well as the right to refuse the treatment or to withdraw consent. [98]

However, informed consent under such terms only provides patients with the right to refuse a diagnostic procedure, a specific treatment or to participate in research, but not the right to object to the use of a particular technology, or to obtain a detailed explanation about the functioning of a certain medical tool or an algorithm. Yet, to take meaningful decisions patients would need at least general information about the technology used, how the algorithm has been constructed and what type of data it uses. Besides, clinicians should explain patients why they have chosen to use that AI system, what its influence is on the diagnosis or treatment, and why they eventually decide (not) to follow its advice; in such a way, patients would be made aware of the contribution the AI had in the final decision. At the moment there are no clear indications in this sense, so that doubts arise on the extent to which clinicians have to inform patients and how detailed information they have to provide them. Therefore, a legislative intervention would be advisable to clarify what kind of information physicians should provide patients when deploying AI systems for diagnostic procedures.

4.2 The MDR Regulation.

Another relevant legislation related to AI in healthcare is the EU Medical Device Regulation (MDR) [99] amending the Medical Device Directive [100] in regulating the use of medical devices within the EU.

The MDR classifies medical devices into four categories (classes I, IIa, IIb, and III) based on their intended purpose and inherent risks. Manufacturers of medical devices shall assess the conformity of their devices prior to placing them on the market and the applicable conformity assessment procedure depends on the classification of the device: for class I devices having a low level of vulnerability the conformity assessment procedure will be carried out under the sole responsibility of the manufacturers; class IIa, IIb, and III devices having a higher risk have to be assessed by an independent accredited certification organisation appointed by the competent authorities of EU Member States.

An important innovation of the MDR is the broader definition of "medical

[97] P Balthazar *et al.*, "Protecting Your Patients' Interests in the Era of Big Data, Artificial Intelligence, and Predictive Analytics" (2018) Journal of the American College of Radiology.
[98] This notion, firstly elaborated in 1957 in a medical malpractice suit, has then been incorporated in several conventions and declarations like the Declaration of Helsinki, the best-known policy statement of ethical principles published by the World Medical Association (WMA) to guide the protection of human participants in medical research, adopted in 1964 and amended seven times, most recently in 2013.
[99] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. The MDR entered into force on May 2017 and entered into application on 26 May 2021.
[100] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices.

devices" that now also includes software used for human beings for the "*Medical purpose of prediction or prognosis of disease as a medical device*".[101] Furthermore, the Regulation specifies that "*software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes is classified as class IIa*".[102] It follows that AI software may be classified under the MDR. For example, Watson for Oncology might be classified at least as a class IIa medical device since it "*provide*(s) *information which is used to take decisions with diagnosis or therapeutic purposes*".[103] This may represent an important step forward in regulating AI-based medical devices because enables medical operators and patients to know that the conformity of medical devices to certain safety standards has been assessed.[104]

4.3 Soft law.

Another important regulatory instrument is soft law, a broad category including a variety of instruments with different characteristics that pose rules of conduct without legally binding force but still producing some legal effects.[105] Two important forms of soft law are co-regulation and self-regulation, based on the intervention of private actors respectively to implement legislative provisions or to regulate private conducts in the absence of legislative provisions.[106]

The use of soft law is still debated among scholars. On the one hand, its main advantages are specificity, that allows to fill regulatory gaps by providing operators with a guidance on how to interpret and apply the legal rules in specific sectors, and flexibility, given that it can easily and rapidly be updated to face new scenarios and new issues. Furthermore, soft law is usually the result of collaboration between public and private actors with the participation of experts; as a result, the drafted provisions are more pragmatic and in line with the needs of a particular sector/processing. On the other hand, some scholars have put forward the risk of "over-saturation"[107] and fragmentation as a result of excessive reliance on soft law and the creation of new instruments for each processing or technology. This would reduce the utility and desirability of these mechanisms by complicating too much the regulatory framework and causing legal uncertainty in an already complex field like AI. In addition, soft law instruments can be effective only when widely adopted, otherwise their regulatory power would be limited lacking strong enforcement mechanisms. A further criticism is that soft law shifts the regulatory power away from the

[101] Art. 2 MDR.
[102] Rule 11 in Chapter III of Annex VIII of the MDR.
[103] S Gerke *et al.*, 'Ethical and legal challenges of artificial intelligence-driven healthcare' (2020) Artificial Intelligence in Healthcare, 295–336.
[104] Annex I of the Medical Device Regulation lists the safety and performance requirements (also including the information to be provided with the device) that medical device must achieve to be released on the market.
[105] L Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?' (2005) 9(1) Electronic Journal of Comparative Law.
[106] *Ibid.*
[107] S Wrigley, 'Taming Artificial Intelligence: "Bots", the GDPR and Regulatory Approaches' in M Corrales, M Fenwick and N Forgó (eds.) *Robotics, AI and the Future of Law. Perspectives in Law; Business and Innovation* (Springer, 2018).

legislature to the private sector or to secondary bodies which lack democratic legitimacy with the risk to make private or commercial interests prevail over those of data subjects.[108]

In the light of this, soft law may still be considered a valuable regulatory instrument provided that it is subject to the control of independent authorities and is used as a complementary tool to give operators a guidance to effectively comply with the (often vague and broad) legal statutory provisions.

An important form of soft law are codes of conduct, a set of rules, ethics or values that guide people/companies/organisations in daily practices, activities, and interactions. In relation to processing of personal data, codes of conduct find a legal ground in Articles 40 and 41 GDPR which analytically describe the procedure of approval and accreditation of such codes;[109] further clarifications have been provided by the EDBP.[110] Adherence to a code of conduct is not mandatory, but several benefits follow its adoption.[111] Also, the use of an approved code of conduct can be used as a basis for a transfer of personal data outside the EU.[112]

The advantages of codes of conduct, especially in a technical sector like genomic diagnostics, are even more relevant in relation to AI since data protection law does not include specific provisions concerning the use of AI-based technologies. Firstly, codes of conduct can be written with the help of practitioners who can better pinpoint the specific needs of healthcare and diagnostics, thus ensuring that data protection issues are addressed accordingly. Besides, their involvement can increase the code's acceptance.[113] Secondly, a code of conduct can formulate best practices and set standards able to harmonise data processing for the entire category of health operators in Member States, thus increasing legal certainty and enhancing patients' trust in AI.[114] Finally, codes of conduct can have a broader scope than legislation and include ethical standards as further safeguards of personal data.[115] As such, geneticists strongly ask for codes of conduct that could help them to overcome

[108] P de Hert, 'The future of privacy. Addressing singularities to identify bright-lines that speak to us' (2016) 3(4) European Data Protection Law Review, 461.

[109] Under Art. 40 GDPR codes of conduct may be drawn up by associations and other bodies representing categories of controllers or processors and then formally approved by supervisory authorities (if the code relates to only one Member State) or the Commission (if the code relates to multiple Member States). After approval codes are collated in a register and made publicly available. The code main purpose is providing data controller and processor with a guidance for processing personal data, especially in relation to the collection of data, the security measures to adopt, the information to provide to data subjects and the ways to make data subjects exercise their rights.

[110] EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.

[111] For example, under Recital 77 and Art. 24(3) adherence to an approved code of conduct can be used by data controller and data processor to demonstrate compliance with the GDPR and, under Art. 83, it can be evaluated by supervisory authorities to mitigate penalties for non-compliance.

[112] Article 46 (2) (e) GDPR.

[113] F Molnár-Gábor, JO Korbel, 'Genomic data sharing in Europe is stumbling—Could a code of conduct prevent its fall?' (2020) 12(3) EMBO Mol Med.

[114] EDPB Guidelines 1/2019 (n 110).

[115] Several codes of conduct have already emerged or are being drafted in the healthcare sector. An example is the Code of Conduct drawn up by the Biobanking and BioMolecular Research Infrastructure aiming to regulate data processing and fostering transparency and trust in the use of personal data for health research within the EU (http://code-of-conduct-for-health-research.eu). In addition, some guidelines are being developed by Alliance Against Cancer for the creation of a technological platform that allows the collection, sharing and analysis of health big data from each Italian research institute (https://www.alleanzacontroilcancro.it/en/commissione-acc-gdpr/).

the gaps and uncertainties left by data protection law[116]. In particular, codes of conduct should address issues like pseudonymisation and standards to ensure adequate data protection, consent and withdrawal, data portability, access, and explainability.[117]

Another accountability tool meant to give data subjects confidence about data controllers' compliance with data processing legal requirements is certification,[118] grounded on Articles 42 and 43 GDPR[119] and addressed by the EDPB in its guidelines.[120]

Although not widespread yet, this instrument may be particularly relevant for AI-based health data processing because patients do not have the knowledge and expertise necessary to fully understand how their data is processed and whether the processing is fair. Hence, the self-determination regime based on the notice-and-consent model cannot ensure an effective protection. On the contrary, certifications would give patients the certainty that the processing is trustable because its compliance to legal provisions and conformity to safety standards has been evaluated by *ad hoc* expert certification bodies.

A further co-regulatory instrument is the data processing impact assessment, a self-assessment procedure through which data controllers and processors, either by themselves or with the help of external bodies, evaluate the impact of data processing.

The rationale behind impact assessment is twofold. [121] On the one hand, the idea that data subjects often cannot fully understand the functioning and the implications of AI-based data processing and cannot take meaningful decisions about the use of their personal data. On the other hand, the acknowledged collective dimension of data protection. The impact assessment would place on

---

[116] In relation to genomic data, major problems in terms of data subjects' identifiability arise because, given the necessity to maintain a strict connection with individual personal genetic profiles, data cannot be anonymised. See M Shabani, L Marelli, 'Re-identifiability of genomic data and the GDPR: Assessing the re-identifiability of genomic data in light of the EU General Data Protection Regulation' (2019) 20(6) EMBO reports. At the same time, large genetic data sets are required to train the algorithms and, considering that genetic diseases are often rare, data needs to be collected and gathered from different data centres around the world with consequent problems of international transfers. See F Molnár-Gábor, JO Korbel, 'Genomic data sharing in Europe is stumbling—Could a code of conduct prevent its fall?' (n 113).

[117] M Philips *et al.*, 'Genomics: data sharing needs an international code of conduct' (2020) 578 Nature, 31 – 33.

[118] Certification has been generally defined by the International Standards Organisation (ISO) as "*the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements*". See https://www.iso.org/certification.html.

[119] Arts. 42-43 GDPR recognise two different certification models. The first model is managed by accredited private certification bodies with an appropriate level of expertise in relation to data protection that can set up a certification scheme and submit it for approval to the competent national supervisory authority or to the EDPB. After approval, the certification body is entitled to manage the conformity assessment and issue the certification when the candidate demonstrates its full conformity with the approved requirements. The second certification scheme is directly set up and managed by national supervisory authorities. In addition, the Regulation allows the establishment of other certification schemes that fall outside the control of supervisory authorities thus giving no certainty about their consistency. The risk is that the proliferation of such unmonitored certification schemes could make people lose trust in certification thus making ineffective the whole system. See E Lachaud, 'What GDPR tells about certification' (2020) 38 Computer Law & Security Review.

[120] EDPB, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation – Revised version 3 (2019).

[121] A Mantelero, 'AI and Big Data: A blueprint for a human right, social and ethical impact assessment' (2018) 34(4) Computer Law & Security Review, 754-772.

the controller/processor, rather than on data subjects, the burden to verify and assess the impact of processing. The results would be made public in order to make data subjects aware of the risks of data uses and able to decide whether or not to accept the processing.

The DPIA set by the GDPR still adopts a risk-based approach focused on data management, data quality, data security and procedural aspects like the regulation of the different stages of data processing and the definition of the powers and tasks of the subjects involved in the process[122]. Yet, there is no reference to the impact on ethical and social values nor on fundamental human rights. This lack is particularly serious for data processing conducted in genomic diagnostics with AI. Indeed, data processing in this field poses high risks for human rights (e.g. the risk of discrimination) and such risks assume a collective dimension given that decision-making is based on clusters created by algorithms. The potential negative impact of data processing is, therefore, no longer restricted to data protection but includes other potential prejudices that can be adequately taken into account only in a broader ethical and social perspective having a collective dimension and based on a human rights assessment.[123]

4.4 Digital ethics.

Finally, the analysis of complementary regulatory instruments could not overlook the social and ethical concerns raised by the use of AI in genomic diagnostics. On this regard, it is first necessary to clarify the role of ethics and how it interacts with data protection law. Albeit data protection legislation maintains a crucial role in regulating data processing and data subjects' rights, when AI comes into play it is no longer sufficient since AI generates radical and irreversible transformative effects that go far beyond data-related issues

[122] Under Art. 35 GDPR the Data Protection Impact Assessment (DPIA) must be conducted when processing "is likely to result in a high risk" to data subjects. The article lists the cases when high risk is presumed and, thus, the DPIA is mandatory. In addition, the A29WP has adopted the Guidelines on performing and evaluating DPIAs which identify nine criteria to evaluate whether the processing results in high risk and the DPIA must be conducted. See Article 29 Working Party WP 248 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 April 2017. Most of these criteria are met in AI-based data processing for genetic diagnostics thus triggering the obligation to conduct the DPIA (in particular, the following criteria are met: automated-decision making with legal or similar significant effect, the processing on large scale of sensitive data also concerning vulnerable data subjects, matching or combining datasets, use of new technological solutions).

[123] Different models have thus been proposed in this direction. The first one is the Privacy, Ethical and Social Impact Assessment (PESIA) adopted by the Council of Europe in its Guidelines on Big Data. This model of assessment has a broader scope than the DPIA in the GDPR, since it also encompasses the societal consequences of data uses and the analysis of their potential conflicts with ethical values. See Consultative Committee of Convention 108, "Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data" T-PD (2017)01, 23 January 2017. A further step forward is the proposed Human Rights, Ethical and Social Impact Assessment (HRESIA), a principle-based model that represents an evolution of the already existing HRIA (Human Rights Impact Assessment) since it combines the assessment of ethical and societal values with the evaluation of the human rights impact. See A Mantelero, 'Towards a Big Data regulation based on social and ethical values. The guidelines of the Council of Europe' (2017) Revista de Bioética y Derecho. See also P de Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in D Wright and P de Hert (eds.) *Privacy Impact Assessment; Law, Governance and Technology* (Springer, 2012) 6.

giving rise to new and broader risks.[124] To mitigate these risks, new solutions need to be implemented with a systemic approach that cannot only rely on hard governance measures. In fact, statutory obligations only indicate what is legal and illegal but, as Floridi notes, they say "nothing about what the good and best moves could be, among those that are legal, to win the game, that is, to have a better society".[125] When it comes to genetic diagnostics, the GDPR regulates data processing in order to ensure data quality and data safety from a legal point of view, but it says nothing on how data should be processed to reach the best result for the patient (e.g. avoiding bias, taking fair therapeutic decisions, preventing false positives or false negatives). It follows that legal compliance is necessary but not sufficient to ensure an adequate balance of the interests at stake and an effective protection of patients' rights. Therefore, it is essential to enhance data protection law with ethical guidelines that support geneticists in processing patients' personal data in accordance with data subjects' expectations, needs, and rights.[126]

To this end reference should be made to "digital ethics" or "data ethics", the branch of ethics that studies moral problems related to data, algorithms and corresponding practices, in order to formulate and support morally good solutions.[127]

In this perspective in 2015 the EDPS established the Ethics Advisory Group to analyse the new ethical challenges posed by digital developments and current legislation, especially in relation to the GDPR.[128] In the same direction the European Commission set out its vision for an "ethical, secure and cutting-edge AI made in Europe"[129] and established the High-Level Expert Group on Artificial Intelligence (AI HLEG) that on 8 April 2019 published the AI Ethics Guidelines,[130] then confirmed by the Commission itself in its White Paper on Artificial Intelligence.[131] The Guidelines set out a framework for achieving Trustworthy AI "seeking to maximise the benefits of AI systems while at the same time preventing and minimising their risks".[132] In particular, Trustworthy AI should be lawful (complying with all applicable laws and regulations), ethical (ensuring adherence to ethical principles and values), and robust (causing no harm). Ethics, thus, is considered as a further element that must be added to legal compliance for the implementation of a trustworthy AI.

The AI HLEG elaborated the basic principles for a trustworthy AI on the ground of the bioethical principles originally developed by Beauchamp and Childress and then re-interpreted in relation to the use of AI.[133] Based on such

---

[124] J Morley, L Floridi, 'An ethically mindful approach to AI for health care' (2020) 395 Lancet, 254-255.
[125] L Floridi, 'Soft ethics, the governance of the digital and the General Data Protection Regulation' (2018) 376 Phil. Trans. R. Soc.
[126] *Ibid*.
[127] L Floridi, M Taddeo, 'What is data ethics?' (2016) 374 Phil. Trans. R. Soc.
[128] EDPS Ethics Advisory Group | Report 2018.
[129] European Commission, Brussels 25.4.18 COM(2018)237 and European Commission, Brussels 7.12.18 COM(2018)795.
[130] AI HLEG Guidelines (n 11).
[131] European Commission, Brussels, 19.2.2020 COM(2020) 65 final, WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust.
[132] AI HLEG Guidelines (n 11) paragraph A.
[133] TL Beauchamp, JF Childress, *Principles of biomedical ethics* (7th edn, Oxford University Press 2013). In particular, the principle of beneficence imposes that AI is developed for the common good and the benefit of humanity; the "non-maleficence" or "do no harm" principle requires avoiding any potential negative

principles, the AI HLEG identified the principles of respect for human autonomy, prevention of harm, fairness, and explicability to ensure that AI systems are developed, deployed and used in a trustworthy manner,[134] and identified seven concrete requirements to implement these principles.[135] Lastly, on 21 April 2021 the Commission published its proposal for a Regulation on a European approach for Artificial Intelligence (the "Artificial Intelligence Act"), the first EU legal framework on AI.[136]

In order to ensure an ethical use of AI, the identified ethical principles should be embedded in the design of AI systems: each element of the system should be "pro-ethically" designed to protect the values and principles of ethics.[137] This means that the whole process, from the development and training of algorithms for diagnostics to their deployment, should be designed in ways that decrease inequality, leave room for human autonomy, ensure explicability and data protection.

The idea of ethics embedded in machines is based on the concept of "value sensitive design" developed by Friedman and Kahn in the late 1980s and early 1990s and claiming that human principles and standards must be considered when planning technology.[138] Actors involved in developing a new technology should identify and incorporate human values into the design and development process in order to limit or eliminate potential problems once the technology has been deployed.[139]

The main issue is the selection of human values to embed in AI-based technologies for genomic diagnostics, namely how and by whom these values should be selected and to what extent they can be universally applicable.[140] Indeed, it is extremely difficult to define shared human values and principles and establish what is good or bad in a given situation, *a fortiori* considering the diverse ethical, social and cultural backgrounds spread around the world. A further criticism is the risk of behavioural manipulation and limitation of human

consequences of misusing AI technologies and any violations of human rights, including the right to the protection of personal data; "autonomy" implies the power to decide, meaning that the right of individuals to make decisions for themselves about the treatment to receive must not be constrained by AI; "justice" may be translated as a requirement for a correct use of AI in such a way to avoid biased data and unfair discrimination, ensure that the benefits of AI are shared equally, and prevent the creation of new harms. A fifth principle has been added with specific reference to AI that is "explicability" (in the twofold sense of intelligibility and accountability) requiring that AI systems must be made as much as possible intelligible and understandable (at least) to experts. See L Floridi *and colleagues*, 'AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28 Minds and Machines, 689–707.

[134] AI HLEG Guidelines (n 11), chapter I, paragraph 2.2.

[135] The seven requirements are: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental wellbeing; and accountability. See AI HLEG Guidelines (n 11), chapter II, paragraph 1.

[136] See Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final. This Proposal falls outside the scope of this paper, thus it will not be further analysed.

[137] J Morley, L Floridi, 'How to design a governable digital health ecosystem' (2019).

[138] B Friedman, 'Value-sensitive design' (1996) 3(6) Interactions, 16–23.

[139] B Friedman, PA Kahn Jr., A Borning, 'Value sensitive design and information systems' in N Doorn, D Schuurbiers, I van de Poel and ME Gorman (eds.), *Early engagement and new technologies: Opening up the laboratory* (Springer, 2013), 55-95.

[140] A Cenci, D Cawthorne, 'Refining Value Sensitive Design: A (Capability-Based) Procedural Ethics Approach to Technological Design for Well-Being' (2020) 26 Science and Engineering Ethics. See also A Gerdes, 'An Inclusive Ethical Design Perspective for a Flourishing Future with Artificial Intelligent Systems' (2018) 9 European Journal of Risk Regulation, 677–689.

free choice. Indeed, when the technological architecture embeds certain ethical values, it nudges users to act according to those values without leaving them any choice.[141]

However, as it has been argued by Vermaas et al., "technical artefacts are not morally neutral because their functions and use plans pertain to the objectives of human actions, and those actions are always morally relevant".[142] This means that technologies are never neutral but always reflect specific values and normative goals. Given that, the main point becomes what values should be reflected in technology and who should fix them. Different suggestions have been put forward.

First of all, *ad hoc* ethical committees may play a crucial role as independent organisms made up of experts in technology, medicine, ethics and bioethics who may support the regulator in identifying the ethical issues raised by AI and the ethical values to be implemented. Several ethical committees have already been instituted by national and international organizations,[143] and both in the public and private sector several AI guidelines and ethical codes of practice have been adopted.[144] In the field of genomic diagnostics mention can be made to the UK-France Genomics and Ethics Network,[145] and the Joint Committee on Genomics in Medicine that published a guide on the ethical issues arising from the use of genetic and genomic information in the clinic.[146]

Other important instruments are codes of ethics which set the ethical values and practices to follow in developing and deploying AI systems for genomic diagnostics.[147]

Finally, a way to select the values to embed in AI systems and develop a pro-ethical design would be to engage all the categories of actors involved

[141] L Floridi, 'Tolerant Paternalism: Pro-ethical Design as a Resolution of the Dilemma of Toleration' (2016) 22 Sci Eng Ethics.
[142] P Vermaas *et al.*, 'A philosophy of technology: from technical artefacts to sociotechnical systems' (2011) 6(1) Synthesis Lectures on Engineers, Technology and Society, 1–134.
[143] Some examples are the HLEG on AI appointed by the European Commission; the expert group on AI in Society of the Organisation for Economic Co-operation and Development (OECD); the Advisory Council on the Ethical Use of Artificial Intelligence and Data in Singapore; the Select Committee on Artificial Intelligence of the UK House of Lords.
[144] Examples are Google's AI Principles; IBM's everyday ethics for AI; Microsoft's guidelines for conversational bots; Intel's recommendations for public policy principles on AI.
[145] The Network has been "set up to reflect on the ethical and social issues arising from the integration of genomics into routine clinical care". See M Gaille, R Horn, The UK-FR GENE (Genetics and Ethics Network) Consortia *et al.*, 'The ethics of genomic medicine: redefining values and norms in the UK and France' (2021) Eur J Hum Genet.
[146] Royal College of Physicians, Royal College of Pathologists and British Society for Genetic Medicine, *Consent and confidentiality in genomic medicine: Guidance on the use of genetic and genomic information in the clinic* (3rd edn. Report of the Joint Committee on Genomics in Medicine. London: RCP, RCPath and BSGM, 2019).
[147] For instance, in 2019 the UK adopted the Code of Conduct for data-driven health and care technologies setting out the behaviours required to those developing, deploying and using data-driven technologies in such a way to balance the benefits deriving from data-driven health and care technologies to patients, clinicians, service users and the system as a whole with issues such as transparency, accountability, liability, explicability, fairness, justice and bias in order to make sure that the health and care system does not cause unintended harm. This Code is based on the Nuffield Council of Bioethics' principles for data initiatives (respect for persons, respect for human rights, participation and accountability). See Nuffield Council of Bioethics, 'The collection, linking and use of data in biomedical research and health care: ethical issues' (2015).

following the model of society-in-the-loop (SITL) developed by Rahwan.[148] According to Rawhan, when AI systems perform a broad function which has wide societal implications, the algorithms should embed the values of the society as a whole.[149] Indeed, when different interests and rights are at stake, trade-offs need to be negotiated and in doing so the regulator should take into account all the parties involved. This means that in regulating the use of AI for genomic diagnostics all the relevant stakeholders, such as patients and healthcare professionals, but also engineers developing algorithms, should not be regarded just as users subject to the rules imposed by the legislator with a top-down approach, but rather as part of the regulatory process. In such a way, they can put forward their interests and express their expectations and concerns around the use of AI with a collaborative approach in order to identify and combine the values expressed by the different players. As such, they should be regularly engaged throughout the whole design process in order to take more widely accepted decisions and build societal trust in AI.[150]

Conclusions.

Over the last years AI has been revolutionising healthcare under several aspects thanks to the development of machine learning and neural networks that are able to elaborate large sets of data, identify patterns and apply them to unseen data. This development has been enabled by big data, namely the possibility to collect and analyse huge amounts of data from a sheer number of individuals around the world. However, the processing of such amounts of data may pose problems in terms of protection of personal data and individuals' fundamental rights. This topic deserves significant attention because even though AI may significantly improve current diagnostic tools based on individuals' genomic profiles, it may also significantly impact on data subjects' rights given the involvement of sensitive data like genetic data. Therefore, effective regulatory instruments must be identified and put in place.

Among those instruments, the GDPR plays a primary role. However, some misalignments have been identified between the Regulation and the development of AI. The reason is that different interests are at stake, often conflicting between each other. On the one hand, there is the need to safeguard individuals against abuses of third parties that would like to gather as much data as possible to build strong algorithms (indeed, the more data algorithms are trained on, the more accurate and effective they are). To avoid any abuses, data protection law sets strict limits such as the principle of data minimisation and purpose limitation, or the requirement of a lawful basis for processing (e.g. data subjects' consent). On the other hand, it must be noted that the development of AI is not negative *per se* but, on the contrary, may have

[148] I Rahwan, 'Society-in-the-Loop: Programming the Algorithmic Social Contract' (2018) 20(1) Ethics and Information Technology, 5–14.
[149] *Ibid.*
[150] To that end, for instance, Involve and DeepMind developed a guidance on stimulating effective public engagement on the ethics of artificial intelligence. For further details see https://www.involve.org.uk/sites/default/files/field/attachemnt/How%20to%20stimulate%20effective%20public%20debate%20on%20the%20ethics%20of%20artificial%20intelligence%20.pdf.

important benefits for the society as a whole. In particular, AI may significantly improve existing diagnostic tools making it possible to detect disease at an earlier stage and intervene earlier with an adequate medical therapy, thus increasing the quality of patients' life. Developing AI in genomic diagnostics, thus, is meant to protect patients, not to exploit them, and provisions that pose too strict limits to the development of AI, impeding or slowing it down, do not necessarily protect patient's rights. Hence, it is necessary to strike a balance between these conflicting interests to allow the development of AI in a safe and respectful fashion.

Based on this conclusion, further legal and non-legal regulatory instruments should be considered to integrate data protection law. Soft law instruments (like certifications, codes of conduct, impact assessment) have been found highly effective to provide *ad hoc* provisions tailored on the specific issues of genomic diagnostics. Yet, there are some side backs as well, like the risk of over proliferation of such instruments leading to legal uncertainty, or the risk that private interests prevail over the public ones. Thus, soft law instruments may be regarded as a valid integration and specification of data protection law without replacing it.

Secondly, data protection should be enlarged with ethical considerations. The focus should be shifted from the quality and safety of data to human rights and from an individual to a group dimension of protection. The EU is already moving in this direction, as shown by the establishment of the AI High-Level Expert Group, the Commission's White Paper on AI, and the recent proposal for the AI Act.

However, this is only a starting point and further steps are expected in the next years to put in practice the principles identified so far. In particular, it is still not clear how to embed ethics in diagnostic machines – thus realising a pro-ethical design of AI – and how to select the human values to be embedded. In addition, an effective way to engage the actors involved in the processing should be found according to the society-in-the-loop model.

In the light of the above, it may be assumed that one of the main challenges for the next years will be enhancing regulatory instruments that take into account the variety of legal, ethical, and social implications of the use of AI in genomic diagnostics. Specifically, such instruments should represent a fair balance between the protection of both individual and collective rights and the development of efficient AI systems.

EJPLT
European Journal of Privacy Law & Technologies • 2021/1 • ISSN 270

Facial recognition: a challenge for Europe or a threat to human rights?

KONSTANTINOS KOUROUPIS
Assistant Professor of European and Data Rights Law
at Frederick University, Cyprus

Abstract

This article deals with the issue of the use of facial recognition, mainly in the European Union. Its purpose is to provide a thorough and coherent analysis of its lawfulness in accordance with the European legislation. Even though there is a concrete legal background provided by European Directives and Regulations, many EU member states apply facial recognition without a solid legal basis. Therefore, the article pursues to offer valid answers to data rights issues that arise. For this purpose, the study is divided into three axes. The first chapter provides a wide analysis of the European legislation which governs the use of facial recognition. Into the second chapter, special emphasis is given to the application of this method at national level. A critical approach is attempted with the aim to define the legal basis and illuminate the legal gaps raised. The third chapter gives an alternative approach of the issue since it demonstrates the wide use of facial technology at international level and its different legal regulation. The final conclusions not only reflect the research's findings but also propose effective safeguards for the lawful application of the facial recognition in order to improve the European digital strategy.

Keywords: Data protection; Digital strategy; facial recognition; GDPR; privacy; Alicem.

Introduction.

A 'Europe fit for the digital age' is one of the top 6 Commission priorities for 2019-2024.[1] It focuses on the development of a high-level digital strategy which puts to the forefront the use of new technologies in order to create new perspectives for businesses, to enhance security and reliability in technology and to gain greater progress in society. As predicted, the EU's digital strategy aims to put new technology to the benefit social good, to produce a fair and competitive digital economy with benefits for both businesses and people and, finally, to bring an open, democratic and sustainable society. All these goals will be achieved by many actions, both at national and European level. One of those actions is the use of artificial intelligence which '*can bring many benefits, such as better healthcare, safer and cleaner transport, more efficient manufacturing, and cheaper and more sustainable energy. The EU's approach to AI will give people the confidence to embrace these technologies while encouraging businesses to develop them*'.[2]

Artificial intelligence consists of performing many functions that were traditionally executed only by humans. Its scope extends to all levels of social life, such as health, transport, business and the economy. It should also be noted that the EU invests significant amounts to increase benefits brought from artificial intelligence to our society and economy. In the White Paper of the European Commission, entitled 'White Paper on Artificial Intelligence- A European approach to excellence and trust'[3] it is explicitly highlighted that artificial intelligence is closely connected with European legislation on human rights, especially in relation to the protection of privacy and data rights. As the possibilities for monitoring and analyzing people's daily habits and actions increase, as indicated in the workplace environment, it is easy to conclude that significant risks arise related to the above issues.

Facial recognition is a representative example of the application of artificial intelligence. According to Opinion 3/2012 on developments in biometric

[1] Further details on European Commission's priorities for 2019-2024 can be found at its official site https://ec.europa.eu/info/strategy/priorities-2019-2024_en.

[2] See more details about the nature, the scope and goals of artificial intelligence at the official site of the European Commission https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en. In addition, see D.Fiott and G.Lindstrom, 'Artificial Intelligence: What implications for EU security and defence?', published by European Union Institute for Security Studies (EUISS), 1 November 2018, pp.1-8. A general approach regarding artificial intelligence can be also found on M.Medeiros, 'Public and Private Dimensions of AI Technology and Security', in the report 'Modern conflict and artificial intelligence', Centre for International Governance Innovation, 1 January 2020, pp.20-25.

[3] The White Paper on Artificial Intelligence was adopted on 19 February 2020 and is available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

technologies of the Article 29 Data Protection Working Party [4] facial recognition is defined as 'the automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorisation of those individuals. It can be executed through various methods, such as video surveillance systems and smartphones, fingerprint readers, vein pattern readers or just a smile into a camera which might replace cards, codes, passwords and signatures. In the White Paper it is emphasized that facial recognition might have two dimensions, identification and authentication of the person. As noted, '*identification means that the template of a person's facial image is compared to many other templates stored in a database to find out if his or her image is stored there. Authentication (or verification) on the other hand is often referred to as one-to-one matching. It enables the comparison of two biometric templates, usually assumed to belong to the same individual. Two biometric templates are compared to determine if the person shown on the two images is the same person. Such a procedure is, for example, used at Automated Border Control (ABC) gates used for border checks at airports*'.

It can be easily concluded that the automated processing of biometric data included in the facial recognition method carries with it risks to privacy and the protection of fundamental rights[5]. Nevertheless, it is a technique that tends to be widely used in several countries, both in Europe and internationally. [6] Therefore, there is a strong interest in examining the special content of facial recognition, especially its legal regulatory framework at EU level (first chapter). Furthermore, we will examine various methods of facial recognition used in certain countries and their legal grounds (second chapter). An additional part of the study is consecrated on the rules that govern facial recognition at international level in order to provide a comparative study of the issues in question (third chapter). Finally, some personal thoughts will be shared regarding facial recognition's legal challenges.

1. The European regulatory framework on facial recognition.

In general, facial recognition is closely related to issues of private life. Privacy has a wide meaning and can take various dimensions.[7] Notably, it includes many terms of physical and social identity of the person, such as the name, the physical, ethical and psychological composition, the right to personal

[4] Article 29 Data Protection Working Party, 00720/12/EN,WP193, Opinion 3/2012 on developments in biometric technologies, adopted on 27th April 2012, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

[5] A thorough analysis of the risks to human privacy due to facial recognition systems can be found in J.A.Lewis and W.Crumpler, 'Questions about Facial Recognition', published by Center for Strategic and International Studies (CSIS), 1 February 2021, pp.1-7, M Carey, Artificial Intelligence Facial Recognition Threat Detection Environment, CreateSpace Publishing, 2018, pp.1-58.

[6] S Ghaffary and R Molla, Here's where the US government is using facial recognition technology to surveil Americans, 10 December 2019, available at https://www.vox.com/recode/2019/7/18/20698307/facial-recognition-technology-us-government-fight-for-the-future.

[7] According to the European Court of Human Rights, privacy constitutes a wide term which cannot be defined exhaustively. See *Niemietz v. Germany* (CC), no 13710/88, ECHR, 16.12.1992, *Costello-Roberts v. United Kingdom* (CC), no 13134/87, ECHR, 25.3.1993.

development and self-determination.[8] In the strictest sense, considering the method by which facial recognition takes place, European legislation on personal data protection applies automatically. In particular, data collected by facial recognition technology is classified as biometric data, as information about facial features is collected, which constitutes 'special categories of personal data', according to the General Data Protection Regulation.[9] The GDPR divides biometric data into two distinct categories: those relating to the physical, physiological human characteristics, such as weight, dactyloscopic data, eye colour, voice and ear shape recognition and those relating to behavioral characteristics of a natural person, such as keystroke analysis, handwritten signature analysis and eye tracking. Both of these categories, allow for and/or confirm the unique identification of that natural person.

Therefore, processing special categories of personal data is lawful if one of the specific conditions of article 9§2 of the Regulation are applied. In that respect, the opinion of European Data Protection Supervisor who proceeds to a thorough legal and ethical examination of facial recognition should be noted.[10] Firstly, there is the aforementioned requirement to meet one of the conditions of Article 9§2 of the GDPR. Then, special emphasis is given to the content of the consent that should be required. Article 7 of the European regulation sets out the nature of the consent: '*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding*'. The question arises as to what extent it is possible to obtain a consent with those elements? How can we be sure that the subject of data gives his consent free and without any reservation?

Furthermore, accountability and transparency should be observed. As it is emphasized, '*it is almost impossible to trace the origin of the input data; facial recognition systems are fed by numerous images collected by the internet and social media without our permission. Consequently, anyone could become the victim of an algorithm's cold testimony and be categorised (and more than likely discriminated) accordingly*'. Regarding this issue, we should add the provisions of the GDPR regarding data protection by design and by default.[11] Under these provisions, '*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*'. In other words, any organization, natural or

[8] See ECHR *Pretty v. United Kingdom* (CC), no 2346/02, ECHR, 29.4.2002, *R.R. v. Poland* (CC), no27617/04, ECHR, 26.5.2011.
[9] Article 9 of GDPR.
[10] W Wiewiórowski, EDPS, 'Facial Recognition: A solution in search of a problem?', 28 October 2019, article available at the official site of the European Data Protection Supervisor https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.
[11] Regarding the privacy by design and by default see article 25 of the General Data Protection Regulation.

physical person who intends to process data rights is encouraged to adopt any necessary, appropriate and useful measure, at the earliest stage of the design of the processing operations as well as to ensure the accomplishment of all conditions demanded for the lawfulness of the processing, according to the article 6 of the GDPR. Additionally, in accordance with the special guidelines on article 25 of the GDPR,[12] '*a technical or organisational measure can be anything from the use of advanced technical solutions to the basic training of personnel, for example on how to handle customer data*'. Furthermore, '*data protection by default' refers to the choices made by a controller regarding any preexisting configuration value or processing option that is assigned in a software application, computer program or device that has the effect of adjusting, in particular but not limited to, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility*'.

The European Data Protection Supervisor seems to be uncertain regarding compliance in relation to the principle of data minimization. As the method of facial recognition itself is not fully accurate and clear, the collection of the necessary data is called into question.

Finally, facial recognition is disputable from ethical point of view as well as its value in a democratic society. The treatment of the human personality as an 'object' clearly violates fundamental human rights, weakening the value of the individual.

For all these reasons, the European Data Protection Supervisor seems to take a more negative stance regarding the use of facial recognition technology, especially since it is often used in respect to vulnerable social groups. Furthermore, he is against automated recognition technologies in public spaces, suggesting their temporary ban. However, without prohibiting facial recognition in an absolute degree, he puts a special burden of responsibility on the national data protection supervisors, who are also called upon to decide on this issue. Hence, this advice sets out his opinion on artificial intelligence which clarifies the safeguards of artificial intelligence with respect to fundamental human rights and recommends national data protection authorities issue specific guidelines on this matter.[13]

In addition to the legal analysis performed by the European Data Protection Supervisor, the processing of personal data by the method of facial recognition shall meet some specific provisions of EU data protection legislation. In that sense, both Article 57§1c of the GDPR and Article 46§1c of Directive 2016/680 require the prior opinion of the national data protection supervisory authority for any measure restricting the protection of personal data. Certainly, the data protection impact assessment is needed in order to demonstrate the dangers to fundamental human rights and freedoms as well as to suggest efficient and appropriate solutions.

The European Union Agency for Fundamental Rights (FRA) seems to

[12] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted by the European Data Protection Board, on 13 November 2019, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

[13] EDPS Opinion on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust, Opinion 4/2020, 29 June 2020, https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf.

approach the issue in question with more criticism. Through a paper published at the end of November 2019 focusing on the fundamental rights challenges involved when public authorities deploy live facial recognition technology for law enforcement purposes[14], FRA expresses the opinion that the use of facial recognition technology by public bodies causes (or can lead to) serious harms to fundamental rights and freedoms. It recognizes that the collection and storage of facial images corresponds to the procession of biometric data which, according to article 9 (2) (g) of the GDPR, the processing of biometric data is only allowed where processing is "necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". Consequently, the use of facial recognition must be lawful, fair and transparent, follow a specific, explicit and legitimate purpose and meet all the necessary provisions of GDPR. Special emphasis shall be given on the strong impact that the collection of facial images might have on the exercise of other fundamental rights, such as the freedom of expression and/or the freedom of assembly since when applied during demonstrations may prevent people from exercising the aforementioned rights. Therefore, that collection should be considered disproportionate or unnecessary. Furthermore, facial recognition systems affect the rights of children and violate certain provisions of both European and international binding legal texts, such as the EU Charter of Fundamental Rights and the UN Convention of the Rights of the Child. According to those texts, the best interests of the child must be a primary consideration in all actions public authorities and private actors take concerning children. Since there is a collection, of sensitive data, their further processing demands stricter necessity and proportionality test, compared to adults, since children are more vulnerable.

In addition, we should underline the Council of Europe's policy regarding the issue of facial recognition. Recently, on 28 January 2021, the Consultative Committee of the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data has issued a set of guidelines on facial recognition technology (FRT), addressed to governments, legislators and the private sector[15]. Those guidelines reaffirm the imperative need to meet the fundamental principles of necessity, proportionality, accuracy, lawfulness, fairness and transparency, as well as all the aforementioned requirements by the European legislation. It is explicitly mentioned that facial recognition systems could be considered as necessary and proportionate only if they intend to prevent an imminent and substantial risk to public security, which should be documented before their application. In that vein, facial recognition used by private companies in uncontrolled environments, like shopping centres, should not be allowed.

In conclusion, it becomes obvious that the European legislation, both at EU level in strict sense but also more widely under Council of Europe's guidelines,

[14]Available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.
[15] Available at https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

sets quite strict requirements for the legality of the application of facial recognition. In this respect, Margrethe Vestager, the European Commission's executive vice president for digital affairs, is very critical regarding this method as it breaches GDPR provisions, especially those for the obtainment of clear consent without any reservation. However, she didn't exclude the possibility of the latter occurring in special occasions, such as in the domain of security, and invited national data authorities to review the legal grounds which will allow member states to make their own domestic decisions.[16] Hence, responding to recommendations of some members of the European Parliament, the EU executive of the European Commission's DG Connect, Mr. Kilian Gross, declared during the European Parliament's Internal Market Committee, which took place recently, that a future ban on the use of facial recognition technology in Europe should not be excluded. Therefore, he highlighted the findings of the White Paper on Artificial Intelligence which are related to the use of facial recognition.[17] It is maybe for this reason that many countries, both in EU and outside, apply facial recognition technology, calling for further and thorough analysis and fair balance of rights.

2. Facial recognition in EU member states.

Despite the fact that facial recognition seems to be contrary to European legislation, at national level this method is often applied in several ways. There are different reasons for its application, such as for reasons of security (in airports), protection of public health or personal entertainment (these issues will be considered in more detail below).

France is the first country in the European Union where biometric data processing techniques are applied via the extensive use of cameras in the city of Nice, following the terrorist attack.[18] Furthermore, with the aim to prevent the expansion of the pandemic due to covid19, French police use cameras with speakers to reprimand people who break coronavirus rules.[19] However, French firm Datakalab whose software is used for video surveillance in many towns in France ensures the protection of personality and personal information as no image is stored or transmitted. In that sense, there is no facial recognition. Certainly, it should be noticed that both European Union and United Nations

[16] T Macaulay, 'Automated facial recognition breaches GDPR, says EU digital chief', 17 February 2020, https://thenextweb.com/neural/2020/02/17/automated-facial-recognition-breaches-gdpr-says-eu-digital-chief/.

[17] S Stolton, 'Commission will 'not exclude' potential ban on facial recognition technology', 3 September 2020, article available at https://www.euractiv.com/section/data-protection/news/commission-will-not-exclude-potential-ban-on-facial-recognition-technology/.

[18] M Meeker, 'Nice has Europe's most sophisticated police surveillance, but it failed to stop a new terror attack', 30 October 2020, available at https://www.telegraph.co.uk/technology/2020/10/30/can-anti-terrorism-tech-protect-french-cities-residents-nice/, N Silbert, 'Vidéoprotection: jusqu'où iront les villes', 9 January 2019, available at https://www.lesechos.fr/idees-debats/editos-analyses/videoprotection-jusquou-iront-les-villes-347536, A Bellier, Nice, 'La ville la plus surveillée de France, pourtant vulnerable', 15 July 2017, available at https://www.ouest-france.fr/societe/faits-divers/attentat-nice/nice-la-ville-la-plus-surveillee-de-france-pourtant-vulnerable-4369155.

[19] E Braun, 'French police use cameras with speakers to shout at people who break coronavirus rules', 8 April 2020, available at https://www.politico.com/news/2020/08/04/french-police-coronavirus-cameras-speakers-shout-391320.

encourage the use of digital tools and new technologies with the aim to fight against Covid19. In any case, it is explicitly declared that any contact tracing and modern digital application shall meet all the safeguards for the respect of fundamental rights, especially of data privacy.[20] Hence, in the EU, member states must adopt a necessary and proportionate data retention policy, which conforms with the European regulation on data rights (GDPR) as well as establishes strong safeguards to prevent stigmatization of infected persons or close contacts of infected persons.

In the context of digitalization of services and e-government, we should highlight that France is the first country in the EU with a facial recognition ID system. In fact, the French government through its law on facial recognition, launched a project called 'Alicem' (Authentification en LIgne CErtifiée sur Mobile).[21] It aims to include facial recognition on users' smartphones to allow them to connect to government services applications. Its primary goal is to provide to French citizens and legal residents with a secure and valid digital identity. According to the *Ministry of Interior,* Alice will comply with the "high" security level defined by the European eIDAS (electronic IDentification, Authentication and trust Services) regulation and is in the process of certification by ANSSI (Agence nationale de la sécurité des systèmes d'information – National agency for information systems security). However, France's data regulator condemns this project as it violates the provisions of the GDPR, in particular those of requiring the consent of the subject.

It should also be noted that the method under consideration has been considered for use at airports for security and crime prevention purposes. However, there is no particular legislation which regulates the legality of the use of facial recognition. The opinion of the French Data Protection Agency (CNIL) is enlightening on these issues, as it provides a clear legal framework under which facial recognition can be considered legitimate.[22] CNIL indicates that the GDPR should govern the application of facial recognition in airports. The principles of necessity and proportionality should be taken into account in order to prevent any damage to public security. Of course, the protection of

---

[20] K Panetta, 'How Technology Can Curb the Spread of COVID-19', 18 May 2020, available at https://www.gartner.com/smarterwithgartner/how-technology-can-curb-the-spread-of-covid-19/, United Nations Division for Public Institutions and Digital Government, '*UN/DESA Policy Brief #61:* COVID-19: Embracing digital government during the pandemic and beyond', 14 April 2020, available at https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-61-covid-19-embracing-digital-government-during-the-pandemic-and-beyond/, E-Health Network, 'Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States', 15 April 2020, available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[21] Ministère de l'Intérieur de la République Française, 'Alicem, la première solution d'identité numérique régalienne sécurisée', 16 December 2019, available at https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee, ' France, First Country in EU With Facial Recognition ID System', 6 October 2019, available at https://www.telesurenglish.net/news/France-First-Country-in-EU-With-Facial-Recognition-ID-System-20191006-0011.html.

[22] A thorough analysis of the issue can be found at the official site of CNIL https://www.cnil.fr/fr/reconnaissance-faciale-dans-les-aeroports-quels-enjeux-et-quels-grands-principes-respecter. Further examination is available at K V Quathem and A Oberschelp de Meneses, 'French Supervisory Authority Releases Strict Guidance on the Use of Facial Recognition Technology at Airports', https://www.insideprivacy.com/data-privacy/french-supervisory-authority-releases-strict-guidance-on-the-use-of-facial-recognition-technology-at-airports/, 21 October 2020.

privacy and the completion of data protection impact assessments are required. Furthermore, all the principles of legal processing of data must be applied, such as those of accuracy, storage limitation, integrity and confidentiality and accountability. CNIL's position regarding obtaining prior valid consent is of great interest. According to the guidance in case, consent should be the legal basis for processing, and thus should meet the requirements for consent under the GDPR. Furthermore, there are some special additions:

- *airports should provide an alternative to individuals who do not consent to the use of facial recognition technology;*
- *airports should also allow individuals to withdraw their consent;*
- *consent should not be tied to or mixed with the acceptance of the terms and conditions of a ticket;*
- *individuals should receive enhanced information about the use of facial recognition technology and its alternative(s); and*
- *facial recognition technology should be used only on individuals who have provided their prior consent (for example, it should blur the picture of other individuals in the background and indicate the control zones).*

In our opinion, the requirement of prior valid consent should be fundamental. In fact, a balance between the right to privacy and the need to prevent criminal acts could be based on the optional use of facial recognition by the passenger. Anyone has the right to opt out and if someone refuses to be scanned, he will have his boarding pass and passport checked manually instead. not necessary for the lawfulness of facial recognition. Apparently, the principle to prior consent is respected and gives an adequate solution to the problem[23].The prior information of passengers could constitute the right legal basis as 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller', according to article 1(e) of the GDPR. Moreover, there is in force the Directive 2016/681, widely known as Directive Passengers Name Record (PNR), which provides for the transfer by air carriers of passenger's name records (PNR) data of passengers of both extra-EU and intra-EU flights.[24] With respect to the protection of fundamental rights of passengers and safeguards to their lawful processing, purposes of security and prevention of criminal acts take precedence. However, comparing the extent of the invasion to privacy by the two aforementioned methods, it can be deducted that is greater and more direct in case of facial recognition. Thus, the requirement of prior valid consent is necessary and cannot be substituted by the prior information.

It becomes obvious that GDPR provisions offer safe guidance for the application of facial recognition. Under those conditions, French courts declared school facial recognition illegal due to the GDPR, regardless of whether or not the prior consent of students had been obtained. CNIL also

[23] Facial recognition technology is already used at many airports in USA. A short but well-structured description and analysis on how is applied can be found on F.Street, 'How facial recognition is taking over airports', article published in https://edition.cnn.com/travel/article/airports-facial-recognition/index.html, 8 October 2019.
[24] Articles 1 and 2 of the Directive.

reaffirmed the decision by drawing attention to alternative less intrusive means, such as badge control.[25] In the same vein, the Swedish DPA has fined a municipality 200 000 SEK (approximately 20 000 euros) for using facial recognition technology to monitor the attendance of students in schools.[26]

However, facial recognition seems to be legitimate and legal for the purposes of public security. Hence, in October 2019, the Swedish Data Protection Authority (DPA) approved its use for criminal surveillance, finding it legal and legitimate (subject to clarification of how long the biometric data will be kept). Similarly, the UK DPA has advised police forces to 'slow down' due to the volume of unknowns – but have stopped short of calling for a moratorium. UK courts have failed to see their DPA's problem with facial recognition, despite citizens' fears that it is highly invasive. In the only European ruling so far, Cardiff's high court found police use of public face surveillance cameras to be proportionate and lawful, despite accepting that this technology infringes on the right to privacy.[27]

In accordance with the aforementioned rationale, Greece has recently issued the presidential decree 75/2020 which authorizes the installation and operation of surveillance systems which capture or record audio or video, in public places.[28] The prevention of criminal acts as well as traffic management that includes dealing with road network emergencies, regulating vehicle traffic, and preventing road accidents are defined as legal grounds for the installation and use of surveillance systems. Furthermore, the principles of justification and proportionality are required. Therefore, sufficient indications are required in order to demonstrate either the present or the possible future commitment of criminal offenses. The contribution of sufficient evidence is justified by the reporting of factual data such as, in particular, statistical or empirical data, studies, reports, testimonies, information on the frequency, type and specific characteristics of crimes committed in a particular area, as well as on the basis of the above elements, probable spread or transfer of crime to another public place. Surveillance is deemed necessary when, in the light of the above facts, a reasonable belief is formed that serious public safety risks are posed in these public areas. The prior authorization of judicial authorities is also necessary in case of public gathering. The data collected are erased 48 hours after the end of the event, unless there are serious reasons for

[25] Further details on this matter can be found in L Pascu, 'French high court rules against biometric facial recognition use in high schools', available at https://www.biometricupdate.com/202002/french-high-court-rules-against-biometric-facial-recognition-use-in-high-schools, 28 February 2020, T Christakis, 'First ever decision of a French court applying GDPR to facial recognition', available at https://ai-regulation.com/first-decision-ever-of-a-french-court-applying-gdpr-to-facial-recognition/, 27 February 2020, O Kagan, 'France Prohibits Use of Facial Recognition Technology to Control School Entry', available at https://dataprivacy.foxrothschild.com/2019/11/articles/european-union/gdpr/france-prohibits-use-of-facial-recognition-technology-to-control-school-entry/, 4 November 2019.

[26] European Data Protection Supervisor, Facial recognition in school renders Sweden's first GDPR fine, available at https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en, 22 August 2019.

[27] A Daly, 'The use of live facial recognition technology through a comparative lens', available at https://infolawcentre.blogs.sas.ac.uk/2020/04/30/the-use-of-live-facial-recognition-through-a-comparative-lens-angela-daly/?fbclid=IwAR2mUlEMu5AHMYPXW_rhx_1vsCMvpfNsji_47GRqqIvWwQyLV_89T1rb9jU, 30 April 2020.

[28] The presidential decree is available (in Greek) at the official site https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/proedriko-diatagma-75-2020-phek-173a-10-9-2020.html (in Greek).

investigation of criminal acts. In that case the period of erasure can be extended up to 15 days.

3. The regulation of facial recognition outside European Union.

Contrary to the strict European Union's regulation on facial recognition and its restrictions, things are not the same at international scope. In China technologies based on artificial intelligence are widely used. Therefore, Facial recognition technology has become an integral part of people's daily life and is applied not only for private purposes (eg for home security or payment solutions) but also for public interest (eg police surveillance systems and traffic controls). Furthermore, many companies and organizations are also using facial recognition to improve their customer experience and increase business efficiencies. That phenomenon is favored by the lack of a relative regulatory framework on data facial rights. Considering that, personal information covers the sense and content of the aforementioned term and is defined as 'information that can identify the individuals and that involves privacy of individuals' under the Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks ('NPC Decision') effective as of 28 December 2012.[29] This definition has known several amendments through specific laws. Special emphasis shall be given on the Cybersecurity Law 2016 which offers, implicitly, a special provision on facial recognition; In particular, according to Article 76 of the CSL, '*'personal information' refers to various kinds of information recorded by electronic or other means which, whether independently or combined with other information, can be used to identify a natural person, including personal biochemical information*', which then implicitly covers personal facial information. In addition, the updated Personal Information Security Specification ('the Personal Information Specification') pointed out the concept of 'sensitive personal information' which can be derived from such procession of data rights and so can cover facial recognition issues. Of course, there are imposed strict restrictions on controllers when processing sensitive personal information, such as encryption when transmitting and storing sensitive personal information and a separate disclosure and consenting process. Since then, Face recognition cameras have been deployed in many parts of China to target security checks in public places, such as subway stations and shopping malls. The Minister of Public Security and Chinese police are using those systems of electronic monitoring of human behavior in streets in order to prevent illegal acts. Furthermore, companies such as ZTE, Dahua and China Telecom propose the adoption of new rules and international standards for the integration of face recognition, video surveillance and license plate registration.[30] However, many concerns have

[29] See more details about the regulation of facial recognition in China in C A Parsa, AI, 'Trump, China and the weaponization of robotics with 5G', The AI Organization, 2019, pp.22-28, 133-137. Also see M Tan, China : facial recognition and its legal challenges, 6 May 2020, published in China: facial recognition and its legal challenges (taylorwessing.com).

[30] According to J Kynge and N Liu, 'From AI to facial recognition: how China is setting the rules in new tech, article published in Financial Times', From AI to facial recognition: how China is setting the rules in new tech | Financial Times (ft.com), 7 October 2020.

been raised regarding the lawfulness of facial recognition. Several Chinese cities have imposed stricter laws and requirements on that technology since there are clear risks for human privacy.[31]

Like China, in USA does not exist any specific regulation on Facial Recognition Technologies. Nevertheless, many states use them for purposes of public interest. The Los Angeles Police Department has widely used, during last decade, facial recognition software via surveillance cameras in order to detect suspects of law infringements.[32] Despite that, many states demonstrate their strong fears about the dangers for human privacy due to the use of facial recognition technology. At this point it should be noticed a controversial facial recognition bill in California which finally didn't come into force since it met a huge criticism. Introduced as Assembly Bill 2261, the bill would provide a framework by which companies and government agencies could legally engage in facial recognition, provided they give prior notice. The utility of facial recognition was never questioned. Especially, in the era of Covid19 the aforementioned technology is widely applied and offers great services in health environment via several measures, such as tracking potential patients of Covid19 via specific masks. However, that method would lead to an uncontrolled and undefined surveillance in the workplace since the prior consent was not necessary. For that reason, many California cities did not finally proceed to the adoption of the bill.[33] According to the latest evolutions, facial recognition technology meets strong criticism at legal level since Portland, Oregon became the first jurisdiction in the country to ban the private-sector use of facial recognition technology in public places within the city, including stores, restaurants and hotels. Through the adoption of specific regulation which will come into force on 1st January 2021 'private entities' will be prohibited from using 'face recognition technologies' in 'places of public accommodation' within Portland, except (1) to the extent necessary to comply with federal, state or local laws; (2) for user verification purposes to access the user's own personal or employer-issued communication and electronic devices; or (3) in automatic face detection services in social media applications.[34]

Russia is another country where facial recognition technology is lawful and is widely used. In particular, in Moscow, a network of 100,000 cameras equipped with facial recognition technology are being used to make sure anyone placed under quarantine stays off the streets.[35] A Russian court

[31] T Qu and Y Xue, 'Chinese cities target facial recognition to curb abuse of personal data, article published in South China Morning Post', Chinese cities target facial recognition to curb abuse of personal data | South China Morning Post (scmp.com), 3 December 2020.
[32] K Rector, R Winton, 'Despite past denials, LAPD has used facial recognition software 30,000 times in last decade, records show', LAPD widely used controversial facial recognition software - Los Angeles Times (latimes.com), 21 September 2020.
[33] S Pont, 'On facial recognition, the U.S. isn't China-Yet', On Facial Recognition, the U.S. Isn't China—Yet - Lawfare (lawfareblog.com), 18 June 2020, R Johnston, 'Facial recognition bill falls flat in California legislature', Facial recognition bill falls flat in California legislature (statescoop.com), 4 June 2020.
[34] See more details on that issue in the article entitled Portland, 'Oregon First to Ban Private-Sector Use of Facial Recognition Technology', published in Portland, Oregon First to Ban Private-Sector Use of Facial Recognition Technology | Privacy & Information Security Law Blog (huntonprivacyblog.com), posted on September 10, 2020.
[35] See further details in P Reevell, 'How Russia is using facial recognition to police its coronavirus lockdown, article published in How Russia is using facial recognition to police its coronavirus lockdown - ABC News (go.com), 30 April 2020.

reaffirmed in its decision the lawfulness of such technology ruling that it does not causes any breach of privacy rights. [36] Certainly, there are several requirements for the conformity of facial recognition with data protection principles. Therefore, the cameras are controlled from a purpose-built coronavirus control centre. Images and personal details of those under quarantine are put on a database so they can be recognised by the cameras. The centre can also be used to monitor social media for 'fake news' on the coronavirus, according to officials, and track international arrivals from virus hotspots. However, serious concerns are raised since Russian national authorities seek to expand facial recognition technology. In particular, many privacy groups and digital rights lawyers allege that the national data protection legislation which enables the undefined procession of data rights for the purposes of protection of public security is unproportioned and incompatible with fundamental rights and freedom. According to those allegations, since there is no judicial or public oversight over the surveillance methods in Russia, including facial recognition, there is a potential infringement of the European Convention of Human Rights, mainly of the article 8 regarding the protection of private life. [37] The principles of proportionality, necessity and accountability are violated so facial recognition should be limited. At this point, it should be noticed that the European Court of Human Rights in Strasbourg has already ruled[38] that Russia's legal provisions governing communications surveillance did not provide adequate safeguards against arbitrariness or abuse, and that therefore a violation took place of Article 8 of the European Convention of Human Rights. Consequently, Moscow's use of facial recognition could be contested at the European Court of Human Rights.

Facial recognition is also legitimate and legal practice in Canada where it has been initially used for purposes of border controls. Therefore, in order to guarantee public and national security, the police authorities proceeded to the expansion of the facial recognition technology without any special requirements for the protection of human privacy. That expansion can be easily explained but not justified by the fact that Canada doesn't have a policy on the collection of biometrics, which are physical and behavioral characteristics that can be used to identify people digitally. Because of that, there are no minimum standards for privacy, mitigation of risk or public transparency, according to the Office of the Privacy Commissioner of Canada's website.[39] Consequently, facial recognition systems can be used. Due to the strong criticism regarding the lawfulness of the technology in case, the Canadian Commissioner of the Office of Privacy has recently outlined necessary actions for privacy and data

36 C Stephens, 'Russia court rules facial recognition technology does not violate privacy rights', article published in Russia court rules facial recognition technology does not violate privacy rights - JURIST - News - Legal News & Commentary, 4 March 2020, Reuters, Russian Court Rules in Favor of Facial Recognition Over Privacy Claims, article published in Russian Court Rules in Favor of Facial Recognition Over Privacy Claims - The Moscow Times, 4 March 2020.

37 See S Zhumatov, 'Russia Expands Facial Recognition Despite Privacy Concerns', article published in Russia Expands Facial Recognition Despite Privacy Concerns | Human Rights Watch (hrw.org), 2 October 2020.

38 *Roman Zakharov v. Russia* (GC), no 47143/06, ECHR, 4 December 2015.

39 H Solomon, 'Canada should stop using facial recognition at border crossings, says legal clinic', article published in Canada should stop using facial recognition at border crossings, says legal clinic | IT World Canada News, 7 October 2020.

protection in an annual report to parliament. Through the emission of two specific recommendations on artificial intelligence and its legal requirements, the Commissioner admits the necessity and the great value of the use of facial recognition platforms, especially in the era of the pandemic due to Covid19. Those platforms offer significant help and support in order to prevent the expansion of the pandemic and to protect public health. Nevertheless, stricter rules governing their use should be adopted in order to guarantee human privacy. In that vein, governments must cooperate with data protection authorities to ensure compliance with legal frameworks in the development and use of AI systems, keeping in mind consequences for human rights.[40]

Conclusions.

The thorough analysis which preceded demonstrated some useful conclusions. First of all, it is evident that European Union's policy on data privacy and artificial intelligence seems to provide more efficient and safe guarantees for the protection of fundamental rights in comparison to relevant international legislations. European Union continues to be the safeguard of fundamental rights and freedoms and consolidates the European area of justice. Regarding the legal treatment of the challenges produced by the rapid and ongoing evolution of the technology, it is clear that the facial recognition constitutes an inherent action of the EU digital strategy. Without any doubt, it includes processing of special categories of personal data. Despite the fact that existing European legislation on data rights could be applied, such as the General Data Protection Regulation, the Directive 2016/680[41] and the Directive PNR, the adoption of specific regulatory frameworks at national level is urgent. Certainly, all safeguards for the protection of fundamental rights must be implemented. However, due to the special nature of facial recognition and the continuous evolution of technology, all EU member states should adopt new laws on this issue. Therefore, national data protection authorities must cooperate and issue safe guidelines which would lead to the later adoption of laws.

Regarding the material scope of the proposed legislative package on facial recognition, it should be noticed that, in accordance with the relevant provisions of the GDPR[42] its use could be legal and legitimate for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security. A typical example of this use of facial recognition systems could be applied at airports, as it has been already

[40] K Pivcevic, 'Government facial recognition policies updated in Canada, Sweden and China', article published in Government facial recognition policies updated in Canada, Sweden and China | Biometric Update, 29 October 2020.
[41] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[42] See Article 2 of GDPR.

thoroughly examined, due to the great extent of security risk and the high risk of criminal acts. Furthermore, due to the rapid expansion of the pandemic caused by Covid19, facial recognition technology could be used for the purposes of protection of public health. In all those cases, the establishment of strict conditions of application of facial recognition is of primary interest. In summary, the duration of use should be defined, the recipients of the act should not be children as well as it must be ordered by national authorities, such as police and judicial authorities. Furthermore, adequate and effective safeguards must be put in place against the abuse of power, in accordance with the European Court of Human Rights. [43] Such adequate and effective safeguards would require prior authorization by the competent Minister. In addition, the lawfulness of the measures should be examined either by a judicial authority or by an independent legal body. Under those specific conditions, facial recognition can meet not only the requirements set out under the European legislation on data rights but also the challenges posed by the EU digital strategy. Otherwise, uncontrolled facial recognition will lead to a new form of Orwellian society where technology will not serve the person but will eliminate human dignity[44].

[43] *Klass v. Germany* (CP), no 5029/71, ECHR, 6 September 1978, *Leander v. Sweden* (CC), no 9248/81, ECHR, 26 May 1987.

[44] Concerns have been already raised about the huge extent of mass surveillance due to face recognitions systems. See Senior, W Andrew, 'Privacy Protection and Face Recognition' in S Z Li, A K Jain (eds.), *Handbook of Face Recognition*, Springer-Verlag London Limited 2011, pp.671-691, J Stanley, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy*, American Civil Liberties Union, 2019, p. 5.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Privacy e utilizzo dei droni in ambito civile.

Privacy and use of drones in non-military sector.

ENRICO DAMIANI
Professore Ordinario di Diritto civile Università di Macerata

Abstract

L'impiego dei droni in ambito civile conduce inevitabilmente l'interprete ad affrontare diverse problematiche di natura prettamente giuridica.
La regolazione dello strumento del drone è caratterizzata da un lato dal perseguimento di standards comuni di sicurezza, connessi a specifici processi di certificazione della conformità, soprattutto alla luce del Regolamento delegato n. 947/201975; dall'altro, dal costante impiego della cd. tecno-regolazione (o regolazione non normativa), che richiede l'inserimento di strumenti tecnici nel sistema operativo, per consentire il rispetto delle regole giuridiche, in un'ottica di parziale esternalizzazione della risposta giuridica, delegata alla normazione tecnica, come già avvenuto in sede di GDPR, grazie all'espresso richiamo in esso contenuto del concetto di privacy by design. The use of drones in the civil area inevitably leads the interpreter to tackle various issues of a purely legal nature.

The regulation of the drone instrument in non-military sector is characterized on the one hand by the pursuit of common safety standards, connected to specific processes of certification of conformity, especially in relationship with the Delegated Regulation no. 947/201975; on the other, by the constant use of the so-called techno-regulation (or non-normative regulation), which requires the insertion of technical tools in the operating system, to allow compliance with legal rules, with a view to partial outsourcing of the legal response, delegated to technical standardization, as already happened in for the GDPR, thanks to the express reference contained therein of the concept of privacy by design.

Keywords: *drone; law; responsibility; privacy.*

Summary: Introduzione. – 1. I droni e i terremoti, tra prevenzione e soccorso. – 2. La normativa in materia di utilizzo di droni in ambito civile. – 3. Droni, privacy e dati personali. – Conclusioni.

Introduzione.

L'impiego dei droni in ambito civile conduce inevitabilmente l'interprete ad affrontare diverse problematiche di natura prettamente giuridica.

Benché i primi casi di utilizzo di tali dispositivi abbiano riguardato il settore militare e gli scopi di polizia[1], detti strumenti stanno attualmente vivendo un percorso di progressiva domesticazione e naturalizzazione, grazie alla loro notevole polivalenza funzionale[2]: le caratteristiche tecniche di cui sono dotati (mobilità nello spazio; dotazione di sensori e dispositivi ad alto tenore tecnologico; visuale prospettica data dall'altezza; dimensioni ridotte; digitalizzazione delle informazioni registrate) li rendono estremamente versatili e suscettibili di essere adoperati negli ambiti più disparati. Proprio con riguardo a queste infinite potenzialità e alle *chance* di crescita e di sviluppo, i mezzi aerei a pilotaggio remoto sono stati definiti una *truly transformation technology*[3], che richiede costante attenzione anche da parte dei legislatori nazionali ed europeo, allo scopo di addivenire ad una regolamentazione adeguata del loro impiego che tenga conto anche delle opportunità di crescita economica e tecnologica[4].

---

[1] P. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, London, 2009.

[2] Coglie efficacemente tale evoluzione E. Palmerini, I droni per uso civile nella prospettiva giuridica: appunti per una sistemazione concettuale e normativa, in Diritto dei droni. Regole, questioni e prassi, a cura di E. Palmerini, M. A. Biasiotti, G. F. Aiello, Milano, 2018, pp. 3-21, spec. p. 5: "Evocati dalla stessa parola "drone" (...), l'aura negativa che circonda l'idea del "killing at a distance" e lo spettro della sorveglianza panoptica hanno finito per seguire la tecnologia negli sviluppi successivi" e p. 7: "Capita ormai in effetti di riscontrare, al posto delle metafore sinistre con ci i droni sono stati spesso descritti, anche immagini benefiche, quali "angeli artificiali", "insetti ecologici" o "messaggeri di pace".

[3] Riga Declaration on remoted piloted aircraft (drones) Framing the future of aviation, Riga, 6 marzo 2015, p. 1: "Drones offer new services and applications going beyond traditional aviation and offer the promis to performe existing services in a more affordable and environmentally friendly way. They are a truly transformational technnology".

[4] Parere n. 207/2014 del Comitato economico e sociale europeo in merito alla Comunicazione della Commissione al Parlamento europeo e al Consiglio - Una nuova era per il trasporto aereo - Aprire il mercato del trasporto aereo all'uso civile dei sistemi aerei a pilotaggio remoto in modo sicuro e sostenibile dell'8 aprile 2014: "1. Conclusioni e raccomandazioni. 1.1. L'Europa è nella posizione ideale per sfruttare i vantaggi offerti dall'espansione del settore dei sistemi aerei a pilotaggio remoto (Remotely Piloted Aerial System, RPAS), con le sue ricadute positive in termini di occupazione e consolidamento del ruolo dell'Europa quale centro di conoscenze per la tecnologia e lo sviluppo. Le possibilità di finanziamento esistenti a livello europeo per le PMI possono stimolare l'ulteriore crescita di questo settore. (...) 1.5. Una condizione fondamentale del ricorso agli RPAS di piccole dimensioni è l'esistenza di norme armonizzate, in particolare per gli operatori di RPAS, in relazione alla sicurezza e alla formazione, nonché di norme e disposizioni adeguate in materia di rispetto della vita privata, protezione dei dati, responsabilità e copertura assicurativa. È quindi necessario definire nuove norme o rafforzare quelle esistenti, applicabili agli usi sia privati che commerciali (...)". In argomento, v. anche Committee on Transport and Tourism, Report on safe use of remotely piloted aircraft systems (RPAS), commonly known as unmanned aerial vehicles (UAVs), in the field of civil aviation (2014/2243(INI)), del 29.5.2015.

Secondo l'Organizzazione internazionale dell'aviazione civile (ICAO[5]), un sistema aereo a pilotaggio remoto (qui denominato "drone") è un insieme di elementi comprensivo di un velivolo a pilotaggio remoto, delle relative stazioni di pilotaggio remoto, dei comandi e collegamenti di controllo oltre a tutti gli altri elementi di sistema che possono essere necessari in ogni momento nel corso di un'operazione di volo[6].

Dal punto di vista lessicale occorre precisare che nei documenti ICAO si fa uso dell'espressione *remotely piloted aircraft system* (RPAS), da tradursi in lingua italiana con "sistemi aeromobili a pilotaggio remoto" (SAPR); le espressioni *unmanned aerial vehicles* (UAVs) e *unmanned aircraft systems* (UAS) hanno un significato più ampio, comprendendo sia gli strumenti monitorati da terra che quelli capaci di volare autonomamente; il termine "drone" è invece solitamente usato solo nel linguaggio comune e non costituisce un'espressione ufficiale[7].

In tale diversificata tipologia di mezzi, gli stessi possono essere raggruppati, sotto il profilo progettuale-costruttivo, in tre categorie: quella dei mezzi progettati e costruiti sin dall'origine come *unmanned aircraft*; quella degli OPV (*optionally piloted vehicles*), che comprende mezzi esistenti nell'inventario dei *manned aircraft*, suscettibili di operare anche in modalità remota; quella, infine, dei mezzi "retrofittati", cioè di *manned aircraft* riconvertiti in *unmanned aircraft*. Molto schematicamente, la gestione del volo degli *unmanned aircraft* può avvenire, a seconda dei casi, sia completamente in automatico secondo modalità operative programmate nel computer di bordo, ovvero tramite il controllo di una stazione remota (con base a terra, su una nave, su un aeromobile *manned*, ecc.), dove una persona o un *team* di persone provvedono al pilotaggio, con onde elettromagnetiche, del mezzo stesso ed alla gestione dei sistemi di bordo.

Ho già fatto in precedenza riferimento alle molteplici possibilità di impiego dei droni in campo civile. La duttilità dello strumento si fonda su tre principali ragioni sostanzialmente riconducibili a tre tipi di vantaggi "strategici": a parità

[5] La Convenzione relativa all'aviazione civile internazionale, stipulata a Chicago il 7 dicembre 1944 è stata resa esecutiva con d.lgs. 6 marzo 1948 n. 616, ratificato con l. 17 aprile 1956, n. 561. Tale Convenzione ha istituito anche l'International Civil Aviation Organization (ICAO) agenzia specializzata delle Nazioni Unite con sede a Montreal, dotata di personalità giuridica internazionale, che costituisce il più importante punto di riferimento a livello mondiale per l'elaborazione della normativa in materia di aviazione civile. Per un'analisi della Convenzione in questione e dei compiti dell'ICAO, sia consentito il rinvio a MALINTOPPI, Considerazioni sugli allegati tecnici alle convenzioni internazionali relative all'aviazione civile internazionale, in Riv. dir. nav., 1951, I, p. 264 ss; MONACO, Le funzioni dell'OACI, in Riv. dir. nav., 1953, p. 257 ss; ID., Le funzioni dell'OACI, in Scritti di diritto delle organizzazioni internazionali, Milano, 1981, p. 403 ss; LATTANZI, Organizzazione dell'aviazione civile internazionale (ICAO), in Enciclopedia del diritto, XXXI/1981, Milano, p. 228 ss.

[6] ICAO, Unmanned Aerial Systems (UAS – Sistemi aerei senza equipaggio), Order Number: CIR328, 2011, glossario.

[7] ICAO, "ICAO Circular on Unmanned Aicraft System (UAS): - unmanned aircraft (UA). "An aircraft which is intended to operate with no person on-board. Note. Model aircraft are excluded from this term"; unmanned aicraft system (UAS). "The combination of unmanned aircraft (UA) and system elements necessary to enable the taxiing, take-off/launch, flight and recovery/landing of UA (...)"; - remotely-piloted aircfaft: "An unmanned aircraft piloted by a licensed pilot situated at a pilot station located remotely from the aircraft (i.e. ground, ship, another aircraft, space) who monitor the aircraft at all times and can respond to instructions issued by ATC, communicates on frequency or via data link as appropriate to the airspace or operation and has direct responsibility for the safe conduct of the aircraft throughout its flight. A remotely-piloted aircraft may possess various types of auto-pilot technology but in any time the pilot can intervene in the management of the flight. This equates to the ability of the pilot of a manned aircraft being flown by its flight management system (FMS) to take prompt control of the aircraft".

di missione, i costi sono inferiori rispetto a quelli sostenuti mediante l'impiego di un aeromobile *manned*; la possibilità di operare, senza rischi per l'equipaggio, in ambienti cosiddetti 3D (*dirty, dull* e *dangerous*); la capacità, per certe tipologie di *unmanned aircraft*, di operare su vaste aree, senza soluzione di continuità, per prolungati periodi di tempo, senza la necessità di rientrare alla propria base per consentire l'avvicendamento degli equipaggi.

Come si è correttamente osservato già qualche anno fa, infatti, "in campo civile, le prospettive di utilizzazione di questi mezzi "senza pilota a bordo" (...) assicurano principalmente due vantaggi: la possibilità di ridurre i costi operativi a parità di prestazioni con i mezzi tradizionalmente pilotati; la possibilità di operare in contesti dove sarebbe estremamente difficile, se non impossibile, assicurare l'incolumità fisica dei piloti (ad esempio, operazioni aeree in zone contaminate da sostanze radioattive o chimiche (...). Anche nel trasporto aereo di merci si stanno aprendo interessanti prospettive di impiego per gli UAV: il colosso americano FedEx sta già infatti ipotizzando di dotarsi di una flotta di UAV destinata a sostituire nelle operazioni cargo parte della sua flotta di aerei tradizionali[8]".

Tra le varie aree di impiego, possono annoverarsi: il settore agricolo, sia per le attività di monitoraggio (in fase diagnostica preventiva di valutazione della capacità del terreno, nell'osservazione dello stato di salute della coltura e nella prevenzione delle criticità e delle malattie; nella capacità, per l'agricoltore, di programmare quantità e tempistiche di interventi di precisione specifici) che di intervento (irrogazione di pesticidi o fertilizzanti) e, più in generale, quello scientifico (studio dei fenomeni atmosferici; controllo della biodiversità); il settore istituzionale e dei pubblici servizi (supporto alle attività di polizia; monitoraggio di centrali nucleari, termoelettriche nonché di oleodotti, gasdotti ed elettrodotti; aerofotogrammetria e rilievo dell'architettura); il settore commerciale (trasporto aereo; distribuzione commerciale) [9] ; il settore ambientale[10].

Di particolare e rilevante impatto è il recente impiego di questi strumenti anche durante la pandemia da Covid-19, tuttora drammaticamente in corso, per monitorare gli spostamenti dei cittadini nei diversi territori comunali in modo da controllare il rispetto delle restrizioni previste dalla decretazione d'emergenza, come espressamente autorizzato dalle apposite note ENAC emesse il 23 ed il 31 marzo 2020, con specifico riguardo alle prescrizioni di cui ai Decreti del Presidente del Consiglio dei Ministri dell'8 e 9 marzo 2020[11].

---

[8] B. FRANCHI, Aeromobili senza pilota (UAV): inquadramento giuridico e profili di responsabilità, I e II parte, in Responsabilità civile e previdenza, 2010, 4 e 6, pp. 732 ss. e pp. 1213 ss., spec. p. 732.

[9] Domino's Pizza ha sperimentato per la prima volta questa singolare modalità di consegna della pizza già nell'agosto 2016 in Nuova Zelanda. Ancora più di recente, nell'agosto 2020 la FAA La Federal Aviation Administration (FAA) ha approvato la certificazione di "vettore aereo" per Amazon, che quindi negli Stati Uniti potrà effettuare consegne ai clienti anche attraverso i droni.

[10] Nell'aprile 2021, Arta Abruzzo ha dato il via al progetto "le Aquile", con cui si è dota di una flotta di aeromobili a pilotaggio remoto con lo scopo di potenziare il servizio di controllo, monitoraggio e vigilanza in ambito ambientale; cfr. https://www.snpambiente.it/2021/04/08/arta-abruzzo-al-via-il-progetto-le-aquile-per-limpiego-di-droni/.

[11] Foglio ENAC prot. n. 32363 del 23/03/2020: "Nell'ottica di garantire il contenimento dell'emergenza epidemiologica "coronavirus," al fine di consentire le operazioni di monitoraggio degli spostamenti dei cittadini sul territorio comunale, prevista dai D.P.C.M. 8 e 9 marzo 2020, si rende necessario procedere a derogare ad alcune previsioni delle disposizioni del Regolamento ENAC "Mezzi Aerei a Pilotaggio Remoto" Edizione 3 dell'11 novembre 2019. Considerate, pertanto, le esigenze manifestate da numerosi Comandi di

1. I droni e i terremoti, tra prevenzione e soccorso.

È noto come, già da alcuni anni, i droni vengano impiegati non solo per la rilevazione dei danni agli immobili conseguenti ad eventi sismici[12], ma anche a fini di salvataggio delle vittime a seguito di calamità naturali[13].

L'utilizzo di metodologie di telerilevamento a bassa quota (LARS, *low altitude remote sensing*) tramite velivoli radiocomandati con telecamere e altri sensori a bordo (di varia natura: ottici, chimici...) consente l'acquisizione di immagini sugli edifici danneggiati dal sisma, pur se le zone in cui essi insistono sono inaccessibili e/o pericolose da raggiungere, specialmente se l'acquisizione di informazioni deve avvenire in situazioni di emergenza. Successivamente le immagini e gli altri dati acquisiti vengono processati mediante un apposito software di elaborazione al fine di evidenziare, tramite procedimenti automatici, il tipo di danno prodotto dall'evento sismico e conseguentemente il tipo di azione da avviare, allo scopo di bloccare un eventuale suo aggravamento e programmare una possibile attività per la messa in sicurezza dell'edificio.

Inoltre, la periodicità dei controlli consente di monitorare i cambiamenti intervenuti e di procedere alle eventuali correzioni delle azioni già intraprese. Un ulteriore vantaggio offerto dall'uso dei SAPR è rappresentato dal fatto che detti dispositivi sono in grado di superare il limite di raggiungibilità delle zone terremotate e riportare il rilievo completo e dall'alto di tutta l'area considerata, non solo delle parti sottostanti agli edifici[14].

L'utilizzo dei vettori a bassa quota avviene quando non sia conveniente o possibile l'impiego di strumenti tradizionali quali un aereo o un satellite, oppure quando sia richiesta un'alta risoluzione del rilievo al suolo, od ancora siano necessarie ispezioni su aree molto piccole, come nel caso di indagini relative ad edifici. Il telerilevamento di prossimità viene attuato con l'utilizzo di UAV (*unmanned aerial vehicles*), ossia di piccoli aeromobili senza pilota a bordo e teleguidati a distanza che sono adatti ad acquisire, a bassa quota e ad alta risoluzione, dettagli architettonici e strutturali dei fabbricati al fine di poter dedurre il loro stato di conservazione, l'entità dei danni subiti ed individuare eventuali pericoli di crollo.

In un'indagine condotta da scienziati dell'ENEA successivamente al terremoto dell'Emilia Romagna del 20 maggio 2012, i voli del droni sono stati effettuati "a vista", previa chiusura dell'area all'accesso di pedoni e veicoli[15] anche al fine di evitare possibili violazioni della privacy o ipotesi di responsabilità civile; questa esperienza è idonea a fornirci il contesto di riferimento nel quale la presente indagine dovrebbe contribuire a fornire elementi per le conseguenze che dette attività possono determinare nell'ambito degli istituti di diritto civile.

Polizie Locali, fino al 3 aprile 2020", si sono stabilite determinate procedure come da documenti disponibili al link https://www.enac.gov.it/news/utilizzo-droni-provvedimenti-governativi-emergenziali.

[12] E. CANDIGLIOTA, F. IMMORDINO e V. COPPOLA, Danni da sisma: dall'acquisizione dati da droni al processing delle immagini, in Archeomatica, n. 2, giugno 2014, p. 12 ss.

[13] R. DUCATO, Droni per il search and rescue in aree valanghive: profili privatistici, in Diritto dei droni. Regole, questioni e prassi, cit., pp. 379-424.

[14] ZAIRA BAGLIONE PAGLIAROLI, Il rilievo con drone nei centri storici, in GEOmedia, 2016, 2, pp. 24-25.

[15] E. CANDIGLIOTA, F. IMMORDINO e V. COPPOLA, op. cit., p. 12 ss.

Sia consentito sin da ora ipotizzare che, in una prospettiva futura, i droni adoperati per finalità di soccorso post-sisma potrebbero essere verosimilmente integrati in una flotta statale ed impiegati in operazioni di ricerca e salvataggio. Tale considerazione non è priva di rilevanza pratica, ma produce importanti effetti in termini di disciplina applicabile ai droni utilizzati per tali scopi: in questo caso infatti, non troveranno applicazione le norme del codice della navigazione, secondo quanto previsto dall'art. 748 cod. nav.[16], trattandosi di una categoria compresa tra quelle esonerate (aeromobili militari, di dogana, delle Forze di polizia dello Stato e del Corpo nazionale dei vigili del fuoco, nonché aeromobili ad essi equiparati *ex lege* di cui all'art. 744 comma 4 cod. nav.).

Inoltre, il Regolamento europeo droni 2018/1139 esclude dal proprio ambito di applicazione, ai sensi dell'art. 2 paragrafo 3 lett. a), i "...dispositivi di controllo remoto impegnati in operazioni militari, doganali, di polizia, di ricerca e salvataggio, di lotta antincendio, di guardia di frontiera e costiera o in attività o servizi analoghi, effettuati sotto il controllo e la responsabilità di uno Stato membro"; di contro, la nuova edizione del Regolamento ENAC acquisisce, in maniera complementare, la competenza ad emanare norme e procedure applicabili anche "agli UAS privati o di Stato che conducono attività che ricadono nelle previsioni dell'art. 2 comma 3 a) del Regolamento (UE) 2018/1139 ma per i quali le competenti Amministrazioni dello Stato non abbiano emesso speciali regolamentazioni di cui all'articolo 748 del Codice della Navigazione". La competenza regolamentare rimane dunque affidata alla disciplina nazionale, sebbene il Regolamento ENAC abbia valenza residuale rispetto alla disciplina specifica prevista per i droni di Stato e assimilati[17].

Una significativa deroga è altresì prevista in tema di rispetto della normativa sulla privacy: nel caso di operazioni di soccorso post-sisma, non sarà necessario ottenere il consenso dell'interessato, alternativamente nelle ipotesi in cui il trattamento sia necessario a) per adempiere ad un obbligo previsto dalla legge (quale il dovere di prestare soccorso), ovvero b) per la salvaguardia della vita o dell'incolumità fisica di un terzo o dell'interessato[18].

In argomento appare interessante richiamare i provvedimenti del Garante Italiano della Privacy, sebbene emanati in risposta a quesiti aventi ad oggetto il diverso tema dell'acquisizione dei dati per il soccorso in montagna tramite l'uso dello smartphone; ciò nonostante, quanto da essi emerge, *mutatis mutandis*, risulta adeguato anche ai fini della presente analisi sulla raccolta dati dei droni in caso di soggetti coinvolti in eventi sismici, atteso che il Garante ha ribadito

---

[16] Art. 748. Norme applicabili. comma 1: "Salva diversa disposizione, non si applicano le norme del presente codice agli aeromobili militari, di dogana, delle Forze di polizia dello Stato e del Corpo nazionale dei vigili del fuoco, nonché agli aeromobili previsti nel quarto comma dell'articolo 744".

[17] Sul regolamento ENAC cfr. R. Lobianco, Mezzi aerei a pilotaggio remoto: brevi osservazioni sul Regolamento ENAC, in Resp. civ. e prev., 2017, p. 2065 e segg.

[18] Art. 6 GDPR Liceità del trattamento: "1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (...)c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; (...)d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Sulle implicazioni in generale del tema della privacy si veda D'Orazio R., Finocchiaro G., Pollicino O., Resta G. (a cura di), Codice della Privacy e Data Protection, Milano, 2021; sul tema specifico, ci sia consentito il rinvio a E. Damiani, L'utilizzo dei droni e le inerenti ricadute sul diritto della privacy e della responsabilità civile, in dimt.it (18 marzo 2021).

.

che "è lecito acquisire dati sulla localizzazione relativi alle persone medesime anche senza il loro consenso se vi è la necessità di salvaguardare la vita o l'incolumità fisica della persona (...)[19]". Si tratta di rilievo più che condivisibile, espressione di un doveroso bilanciamento di interessi [20], che considera prevalente, in una situazione emergenziale, l'incolumità fisica dell'interessato rispetto alla tutela della riservatezza e dei propri dati personali.

Dal punto di vista pratico ed applicativo, la possibilità di eseguire rilievi attraverso i droni, soprattutto per il monitoraggio del territorio in situazioni di emergenza, rappresenta una conquista importante ai fini della stima dei danni causati da calamità naturali, oltre che nella potenziale ottica dell'attività di prevenzione.

Già a seguito delle tragiche vicende relative al terremoto che ha colpito l'Abruzzo il 6 aprile 2009, nell'ambito di un Progetto di Ricerca Nazionale[21], l'Università degli Studi dell'Aquila ha dato avvio all'impiego della tecnologia SAPR in alcune zone colpite dal sisma, al fine di evidenziare le criticità e monitorare lo stato degli edifici, tenendo in considerazione altresì gli aspetti inerenti la prevenzione delle emergenze e l'innovazione delle metodologie di telerilevamento. Nella pratica, l'utilizzo di questo nuovo metodo di rilievo tramite drone ha consentito agli operatori di raggiungere zone e punti altrimenti inaccessibili, ottenendo risultati di maggiore dettaglio a completamento ed integrazione delle informazioni già raccolte con gli strumenti topografici tradizionali.

La coordinatrice del progetto di topografia e APR nel centro storico aquilano, promosso dalla Università degli Studi dell'Aquila ha dichiarato che "questo progetto ha rappresentato una sfida perché, per la prima volta, in Italia un progetto di ricerca ha avuto come oggetto un centro storico cittadino. La fotogrammetria da UAV ha il vantaggio di integrarsi perfettamente con le altre tecniche di rilievo, inoltre l'applicazione di sensori diversi a seconda delle esigenze del momento può portare ad ottenere fotogrammi migliori e quindi prodotti finali di qualità ancora più alta. Nel futuro questa esperienza potrebbe essere riproposta per rilanciare l'edilizia nazionale (...)[22]".

Anche a seguito del terremoto che ha colpito Lazio, Abruzzo, Marche e

[19] Si tratta in particolare del Provvedimento "Persone disperse in montagna: si può localizzare il cellulare per rintracciarle", 19 dicembre 2008 e del Provvedimento "Utilizzo di tecnologie di geolocalizzazione di persone infortunate o disperse in montagna da parte del Corpo Nazionale Soccorso Alpino e Speleologico (CNSAS)" del 22 gennaio 2015.

[20] Sul bilanciamento degli interessi si veda da ultimo G. Perlingieri, Ragionevolezza e bilanciamento nell'interpretazione recente della Corte costituzionale, in Riv. dir. civ., 2018, p. 716 ss.

[21] La ricerca è stata avviata nel 2011 e finanziata dal Miur con l'obiettivo di definire le strategie innovative per il telerilevamento e mappatura webgis del rischio in tempo reale e la prevenzione del disastro ambientale. Diretta a livello nazionale dal Prof. Raffaele Santamaria dell'Università degli Studi di Napoli Parthenope, la ricerca ha raggruppato circa 10 unità locali, in particolare l'unita dell'Aquila si è impegnata nella valutazione dell'impatto del sisma nel centro storico, nella Piazza Palazzo e nella Basilica Collemaggio e anche in altri comuni limitrofi.

[22] Z. Baglione Pagliaroli, Il rilievo con drone nei centri storici, cit., p. 26.

Umbria del 24 agosto 2016[23], nell'ambito del progetto TRADR[24] finanziato dall'Unione Europea, sono state monitorate le condizioni delle Chiese di San Francesco e Sant'Agostino, site in Amatrice, due tra gli edifici più colpiti dagli effetti del terremoto. Nello specifico, si è fatto un uso sinergico di tre droni: mentre uno di essi si accingeva ad entrare all'interno della struttura, gli altri due erano pronti a fornire indicazioni e punti di riferimento da altre visioni prospettiche, in modo tale da permettere agli operatori di capire come muoversi in sicurezza anche nei punti più pericolosi. L'ingegnere dei vigili del fuoco che ha controllato le operazioni sopra descritte, ha ribadito che "in una situazione del genere, con tutte queste macerie, un'autoscala non potrebbe arrivare. Il drone è il mezzo più idoneo e garantisce un grado di dettaglio molto elevato[25]".

Quanto al secondo profilo, pur ancora in fase sperimentale ed esplorativa, si dà atto degli incoraggianti risultati ottenuti da un team di scienziati italiani ed inglesi coordinato da Alessandro Tibaldi, del Dipartimento di Scienze dell'Ambiente e del Territorio e di Scienze della Terra dell'Università di Milano-Bicocca, che in già in Islanda e in Grecia hanno impiegato tale tecnologia per analizzare le faglie che potrebbero generare terremoti. Ciò è stato possibile grazie alla programmazione da terra di un drone dotato di un sistema Gps di navigazione satellitare e di strumenti di ripresa ad alta risoluzione a diversa lunghezza d'onda (quali fotocamere "standard" e fotocamere termiche per gli infrarossi), in grado di sorvolare a bassa quota l'area di interesse e di ricostruire dettagliatamente - nell'ordine di grandezza dei centimetri - la topografia e la geologia del territorio, con una precisione impossibile da raggiungere con altri sistemi, compresi elicotteri e satelliti artificiali, grazie alla maggiore vicinanza al suolo e alle modeste dimensioni di cui è caratterizzato il drone. Alessandro Tibaldi ha dichiarato che mentre "In Islanda le riprese hanno compreso un territorio abbastanza pianeggiante, in Grecia invece ci troveremo in presenza di pareti rocciose verticali alte centinaia di metri e spesso instabili (...) Si apriranno certamente nuovi orizzonti di indagine in località finora difficili o impossibili a studiarsi[26]".

Da un punto di vista strettamente giuridico, non sembra che a tali tipologie di droni possa farsi applicazione del Reg. UE 1139/2018, in virtù della clausola di esonero contenuta nell'Allegato I al predetto regolamento, che

[23] In argomento, v. anche https://www.interno.gov.it/it/notizie/i-droni-supporto-operazioni-soccorso-dei-vigili-fuoco: "Aeromappature, ricostruzione in 3D del territorio, attività di ricerca in edifici pericolanti. I droni hanno trovato ampio utilizzo durante gli interventi di soccorso dei Vigili del fuoco, nel Centro Italia, a seguito del sisma del 24 agosto scorso. Dall'inizio dell'emergenza i Sapr (Sistemi aeromobili a pilotaggio remoto) del Corpo hanno effettuato circa 9 ore di volo per l'acquisizione di immagini e video. Per tale attività sono stati impiegati droni ad ala fissa ed ala rotante. Questi ultimi, per caratteristiche tecniche, sono stati utilizzati per produrre immagini e video sia delle operazioni di soccorso che dei luoghi colpiti dal sisma. I Sapr ad ala rotante, inoltre, sono stati utilizzati nelle attività di ricerca in edifici pericolanti e per verifiche puntuali in contesti pericolosi o a elevato sviluppo verticale".

[24] Progetto TRADR (Long Term Human Robot Teaming for Robot Assisted Disaster Response) della Commissione europea, un progetto a cui aderiscono venti istituti di ricerca europei, compresa l'università La Sapienza di Roma. TRADR non nasce per i terremoti ma piuttosto per gli interventi dopo i grandi disastri industriali, ma è molto utile anche in caso di calamità naturali dal momento che può entrare negli edifici pericolanti prima dei soccorritori, e capire se la struttura è abbastanza salda da consentire l'accesso a tecnici e squadre SAR.

[25] Così i droni stanno aiutando l'Italia a rimettersi in piedi dopo i terremoti, in www.dronezine.it; https://www.dronezine.it/34699/cosi-droni-stanno-aiutando-litalia-rimettersi-piedi-terremoti/.

[26] https://www.teknoring.com/news/ingegneria-civile/prevenzione-terremoti-arrivano-i-droni-anti-sisma/.

espressamente esclude dal proprio ambito di applicazione gli aeromobili specificatamente progettati o modificati per scopi di ricerca, sperimentazione o scientifici[27].

2. La normativa in materia di utilizzo di droni in ambito civile.

Prima di procedere all'individuazione e all'analisi della normativa relativa all'impiego dei droni in ambito civile, si ritiene necessario circoscriverne il concetto, al precipuo scopo di stabilire quali siano le inerenti ricadute sulla tutela della *privacy*. Tali operazioni analitiche ed ermeneutiche sono rese più complesse dal fatto che il contesto normativo nel quale si colloca l'argomento oggetto di analisi è molto frammentato e soggetto a continue evoluzioni.

Ebbene, ponendo l'attenzione in ambito eurounitario, si segnala che l'Unione europea ha da diversi anni avviato un processo di monitoraggio del fenomeno degli *unmanned aircraft*, adottando una strategia volta ad implementare in Europa la crescita del mercato dei predetti mezzi, definitivamente e formalmente approvata con la "*Riga declaration on remotely pilote aircraft (drones) "framing the future of aviation*[28]" del 6 marzo 2015, significativamente definita il "manifesto[29]" dell'Unione Europea in materia di droni. La predetta Dichiarazione contiene i seguenti principi, qui sinteticamente riproposti, che hanno costituito le linee guida per l'elaborazione della normativa specifica in argomento da parte dei competenti organi dell'Unione europea: 1. I droni devono essere considerati come un nuovo tipo di aeromobili con regole proporzionate basate sul rischio scaturente da ciascuna operazione; 2. L'Unione Europea dovrebbe sviluppare sin da ora regole adeguate per la sicurezza dei servizi svolti con questi strumenti; 3. Devono essere sviluppati tecnologie e standard adeguati alla piena integrazione dei droni nello spazio aereo europeo; 4. L'accettazione dei droni da parte della collettività costituisce la chiave per lo sviluppo dei servizi aventi ad oggetto tali strumenti; 5. L'operatore del drone è responsabile del suo utilizzo[30].

Il Regolamento CE n. 1592/2002 [31] recante regole comuni nel settore

---

[27] ALLEGATO I - Aeromobili di cui all'articolo 2, paragrafo 3, lettera d) 1. Categorie di aeromobili con equipaggio ai quali il presente regolamento non si applica: (...)b) aeromobili specificatamente progettati o modificati per scopi di ricerca, sperimentazione o scientifici e suscettibili di essere prodotti in un numero molto limitato". Sebbene l'allegato sia riferito agli aeromobili con equipaggio, lo scopo di ricerca scientifica o comunque sperimentale potrebbe giustificare un esonero analogo anche nel caso di impiego di aeromobili a pilotaggio remoto.

[28] Il predetto documento è stato adottato il 6 marzo 2015 a Riga, in occasione della conferenza sugli RPA organizzata dal Ministero dei Trasporti della Lettonia, in collaborazione con la Commissione europea. Il testo della Dichiarazione è disponibile in lingua inglese al link https://ec.europa.eu/transport/sites/transport/files/modes/air/news/doc/2015-03-06-drones/2015-03-06-riga-declaration-drones.pdf.

[29] B. FRANCHI, L'evoluzione della normativa internazionale e UE relativa agli "unmanned aircraft", detti anche "droni": profili ricognitori, in Responsabilità civile e previdenza, 2018, 6, pp. 1788-1810, spec. p. 1804.

[30] "1. Drones need to be treated as new types of aircraft with proportionate rules based on the risk of each operation. 2. EU rules for the safe provision of drone services need to be developed now. 3. Technologies and standards need to be developed for the full integration of drones in the European airspace. 4. Public acceptance is key to the growth of drone services. 5. The operator of a drone is responsible for its use".

[31] Regolamento (CE) n. 1592/2002 del Parlamento Europeo e del Consiglio del 15 luglio 2002 recante regole comuni nel settore dell'aviazione civile e che istituisce un'Agenzia europea per la sicurezza aerea, 7.9.2002, L 240/1.

dell'aviazione civile e che istituisce un'Agenzia europea per la sicurezza aerea, datato 15 luglio 2002, ha costituito la prima versione del cd. "Regolamento basico"; già nel Considerando 1 del predetto atto normativo si è dato atto dell'esigenza di "garantire un livello elevato ed uniforme di sicurezza per i cittadini europei nel settore dell'aviazione civile mediante l'adozione di regole di sicurezza comuni e mediante misure per garantire che i prodotti, le persone e le organizzazioni nella Comunità rispettino tali regole e quelle adottate in materia di protezione dell'ambiente"; ciò, al fine di "agevolare la libera circolazione di merci, persone e organizzazioni nel mercato interno[32]". Inoltre, il capo III del predetto Regolamento, in attuazione del Considerando 11[33], ha previsto l'istituzione dell'Agenzia europea per la sicurezza aerea, l'EASA (inizialmente *European Aviation Safety Agency* e ora *European Union Aviation Safety Agency*). All'EASA[34], che costituisce il fulcro della strategia dell'Unione Europea per la sicurezza aerea, sono stati affidati specifici compiti regolatori ed esecutivi sulla sicurezza aerea allo scopo di promuovere i più alti standard comuni di sicurezza e protezione ambientale nell'aviazione civile: essa elabora norme comuni in materia di sicurezza e ambiente a livello europeo, monitora l'attuazione delle norme attraverso ispezioni negli Stati Membri e fornisce le competenze tecniche, la formazione e la ricerca necessarie, collaborando con le competenti autorità nazionali che continuano a svolgere numerosi compiti operativi, come la certificazione di singoli aeromobili o la licenza di piloti.

Con specifico riguardo ai mezzi aerei a pilotaggio remoto, il predetto Regolamento si era limitato ad attribuire all'EASA (ai sensi del combinato disposto dell'art. 4 par. 2 e dell'Allegato II del medesimo regolamento[35]) la limitata competenza a disciplinare i soli aeromobili non pilotati aventi massa operativa superiore a 150 kg, attribuendo per l'effetto agli Stati membri la

[32] Testo consultabile in lingua italiana sul sito eur-lex.europa.eu, al link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L:2002:240:TOC

[33] "È ampiamente riconosciuta la necessità di migliori soluzioni in tutti i settori considerati dal presente regolamento, con la conseguenza che determinati compiti attualmente svolti dalla Commissione o a livello nazionale dovrebbero essere espletati da un singolo organismo specializzato. Occorre pertanto, nell'ambito della struttura istituzionale della Comunità e dell'equilibrio dei poteri esistenti, creare un'Agenzia europea della sicurezza aerea che sia indipendente per le questioni tecniche e sia dotata di autonomia giuridica, amministrativa e finanziaria. A questo scopo è necessario e opportuno che tale Agenzia sia un organismo della Comunità dotato di personalità giuridica e che eserciti i poteri esecutivi conferitigli dal presente regolamento".

[34] Per approfondimenti, si rimanda al sito ufficiale dell'Agenzia: https://europa.eu/european-union/about-eu/agencies/easa_it. Tra i compiti spettanti all'EASA, si annoverano i seguenti: armonizzare regolamentazioni e certificazioni; sviluppare il mercato unico dell'aviazione dell'UE; elaborare norme tecniche nel settore dell'aviazione; certificare aeromobili e componenti; approvare le organizzazioni che provvedono alla progettazione, fabbricazione e manutenzione dei prodotti aeronautici; effettuare controlli di sicurezza e fornisce sostegno ai paesi dell'UE (ad esempio in materia di operazioni di volo e della gestione del traffico aereo); promuovere norme di sicurezza europee e mondiali; collaborare con i soggetti interessati a livello internazionale per migliorare la sicurezza in Europa (ad esempio attraverso l'"elenco per la sicurezza aerea dell'UE" - un elenco degli operatori soggetti a divieto operativo). Le competenze dell'EASA sono state progressivamente ampliate sia dal Regolamento CE n. 216/2008, sia dalla nuova versione n. 1139/2018, a fronte della quale si è reciprocamente assistito ad una corrispondente riduzione delle competenze delle autorità nazionali in tema di aviazione civile (in Italia, deve farsi riferimento all'ENAC, Ente nazionale per l'aviazione civile, istituito con d.lgs. 25 luglio 1997 n. 250).

[35] Articolo 4 Principi fondamentali e applicabilità. (...) 2. Il paragrafo 1 non si applica agli aeromobili di cui all'allegato II". ALLEGATO II - Aeromobili di cui all'articolo 4, paragrafo 2: "Gli aeromobili cui non si applica l'articolo 4, paragrafo 1, sono quelli per i quali non sono stati emessi certificati del tipo o certificati di aeronavigabilità ai sensi del presente regolamento e delle relative regole di attuazione, e che rientrano in una delle seguenti categorie: (...) g) aeromobili non pilotati con massa operativa inferiore a 150 kg".

residua competenza circa la regolamentazione dei droni dotati di massa inferiore al predetto valore.

Tale Regolamento è stato successivamente abrogato e sostituito dal Regolamento CE n. 216 del 2008[36] del Parlamento europeo e del Consiglio del 20 febbraio 2008, che però si è limitato a ribadire la limitata competenza dell'EASA in materia di SAPR aventi massa massima al decollo superiore a 150 kg[37], al fine di garantire una disciplina uniforme, a garanzia dell'incolumità dei terzi e della sicurezza del volo. In attuazione di tale riparto normativo tra la competenza UE e quelle nazionali, in Italia è stato emanato dall'ENAC il regolamento "Mezzi aerei a pilotaggio remoto", la cui prima edizione risale al 16 dicembre 2013, al fine di disciplinare le sole operazioni SAPR di competenza nazionale, cioè "i SAPR di massa massima al decollo non superiore a 150 kg e tutti quelli progettati o modificati per scopi di ricerca, sperimentazione o scientifici[38]".

Questa distinzione, basata sul solo criterio della MTOT, era stata percepita sin da subito come arbitraria ed inadeguata, essendo di contro ritenuto necessario addivenire all'elaborazione di un quadro normativo comune anche per i droni con massa operativa inferiore ai 150 kg, i quali - ad oggi - costituiscono anche quantitativamente la parte più numerosa e rilevante del mercato[39]. Tale esigenza era stata ravvisata anche in ambito UE, laddove si era rilevato che "l'ambito di competenza dell'AESA ristretto ai velivoli senza equipaggio con un peso superiore a 150 kg in base ai principi di aeronavigabilità tradizionali rappresenta un limite arbitrario e dovrà essere riconsiderato[40]".

L'EASA ha pubblicato il 6 febbraio 2018 l'Opinion n. 01/2018[41], recante il titolo *Introduction of a regulatory framework for the operation of unmanned aircraft systems in the "open" and "specific" categories*, un importante documento a carattere innovativo e propulsivo, allo scopo di creare un nuovo quadro normativo unico europeo per la regolamentazione degli *unmanned aircraft*: al suo interno, si dà atto della necessità di estendere la competenza dell'Agenzia a tutte le tipologie di droni, "*regardless of their maximum take-off masses (MTOMs)*".

L'Opinion ha avuto il merito di suddividere le operazioni espletate dai droni in due macrocategorie, denominate rispettivamente *open category* e *specific category*. La categoria "aperta", che ricomprende tutte le operazioni condotte

[36] Regolamento (CE) n. 216/2008 del Parlamento europeo e del Consiglio del 20 febbraio 2008 recante regole comuni nel settore dell'aviazione civile e che istituisce un'Agenzia europea per la sicurezza aerea, e che abroga la direttiva 91/670/CEE del Consiglio, il regolamento (CE) n. 1592/2002 e la direttiva 2004/36/CE, 19.3.2008, L 79/1

[37] Articolo 4 Principi fondamentali e applicabilità 4. Il paragrafo 1 non si applica agli aeromobili di cui all'allegato II. ALLEGATO II - L'articolo 4, paragrafi 1, 2 e 3 non si applica agli aeromobili che rientrano in una o più delle seguenti categorie: (...) i) aeromobili non pilotati con massa operativa non superiore a 150 kg.

[38] Art. 2, Regolamento Enac Mezzi aerei a pilotaggio remoto, Edizione 1 del 16.12.2013, N. 42/2013.

[39] E. PALMERINI, I droni per uso civile nella prospettiva giuridica: appunti per una sistemazione concettuale e normativa, cit., p. 13: "In ragione di questa norma, la stragrande maggioranza delle applicazioni civili e commerciali dei sistemi a pilotaggio remoto ricade nei regimi nazionali, con le conseguenze negative in termini di frammentazione e complessità della disciplina già evidenziate. (...) E' perciò in discussione una modifica del Regolamento di base in materia di aviazione civile che estenda la competenza di EASA (...) che, una volta ampliato il suo raggio di intervento, potrà costituire la base giuridica uniforme per tutto il settore".

[40] Comunicazione della Commissione al Parlamento Europeo e al Consiglio 207/2014 dell'8 aprile 2014 - Una nuova era per il trasporto aereo Aprire il mercato del trasporto aereo all'uso civile dei sistemi aerei a pilotaggio remoto in modo sicuro e sostenibile.

[41] https://www.easa.europa.eu/document-library/opinions/opinion-012018.

con droni con un MTOM inferiore a 25 kg, sotto un'altezza di 120 metri e in VLOS (costante contatto visivo diretto del drone da parte dell'operatore), è suddivisa in tre sottocategorie: A1 (voli su persone ma non su assemblee di persone all'aperto); A2 (voli vicini alle persone nel rispetto della distanza di sicurezza); A3 (voli lontani dalle persone); considerato il basso livello di rischio connesso con lo svolgimento di tali operazioni, non è richiesta né un'autorizzazione preventiva da parte dell'autorità competente, né una dichiarazione dell'UAS prima dell'espletamento dell'operazione. Di contro, la categoria "specifica", stante il maggiore livello di rischio, richiede un'autorizzazione preventiva da parte dell'autorità competente, eccezion fatta per alcuni scenari standard per i quali è sufficiente una dichiarazione dell'operatore.

Lo spartiacque normativo è comunque definitivamente venuto meno con il Regolamento n. 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, il cd. "Nuovo Regolamento Basico" (New Basic Regulation)[42]; esso è entrato in vigore il 1^ luglio 2020, ma al suo interno è previsto un periodo transitorio di 2 anni (2020-2022) durante il quale i droni già in uso senza il nuovo marchio CE potranno volare nelle *limited open category*.

Il Considerando 26 mette in evidenzia il venir meno del riparto delle categorie dei droni in base al peso: "poiché anche gli aeromobili senza equipaggio utilizzano lo stesso spazio aereo degli aeromobili con equipaggio, il presente regolamento dovrebbe disciplinare aeromobili senza equipaggio indipendentemente dalla loro massa operativa"; tuttavia, come di contro chiarito dal Considerando 27, l'Unione è ben consapevole dell'impossibilità di provvedere ad una regolamentazione puntuale e specifica di ogni aspetto, anche "al fine di attuare un approccio basato sul rischio e il principio di proporzionalità"; pertanto, ritiene opportuno "lasciare un certo margine di flessibilità agli Stati membri per quanto riguarda le operazioni di aeromobili senza equipaggio, tenendo conto delle diverse caratteristiche locali nell'ambito di ciascuno Stato membro, quali la densità di popolazione, garantendo al tempo stesso un adeguato livello di sicurezza".

In generale, in capo alle *Autorithies nazionali*, prive della potestà regolamentare, rimangono comunque le funzioni di *oversight* e di controllo, oltre al diritto di designare gli spazi aerei e di interdire il sorvolo di determinate zone del proprio territorio.

In attuazione rispettivamente degli artt. 58 e 61 e dell'art. 57 del regolamento droni del 2018, sono stati pubblicati, nella Gazzetta Ufficiale dell'Unione Europea dell'11 giugno 2019, il Regolamento delegato (UE) 2019/945 della Commissione del 12 marzo 2019 e il Regolamento di esecuzione (UE) 2019/947 della Commissione del 24 marzo 2019.

All'interno dei predetti testi normativi, in parziale attuazione dell'Opinion n. 1/2018 - e a monte del precedente documento, la NPA 2017-05[43] pubblicato

[42] Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio del 4 luglio 2018 recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio, 22.8.2018, L 212/1

[43] https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2017-05.

dalla stessa EASA il 4 maggio 2017 e nel quale le operazioni svolte con l'uso dei droni erano state suddivise in tre e non in due categorie, mediante l'inserimento anche della cd. "*certified" category*[44] - le operazioni UAS sono suddivise nelle categorie "aperta", "specifica" e "certificata", secondo il disposto degli artt. 3, 4, 5, 6 del Reg. 947/2019 e nel rispetto delle prescrizioni di cui all'allegato "Operazioni UAS nelle categorie "aperta" e "specifica". Le operazioni certificate di cui all'art. 6, che prevedono alternativamente il sorvolo di assembramenti di persone, il trasporto di persone o di merci pericolose, richiedono la certificazione del dispositivo e dell'operatore UAS, in uno con il rilascio della licenza al pilota remoto.

La categoria Open comprende 3 sottocategorie (A1, A2 e A3), articolate in 5 classi di aeromobili con caratteristiche diverse che variano da C0 a C4, a cui si aggiungono i droni autocostruiti: rientrano nella sottocategoria A1 i droni di classe C0, C1 e i droni autocostruiti senza marchio CE con peso inferiore a 250 g; appartengono alla sottocategoria A2 gli aeromobili di classe C2 ed, infine, alla sottocategoria A3 le classi C3, C4 e i droni autocostruiti con peso inferiore a 25 kg privi di marchio CE. Conseguentemente i droni, per poter volare in categoria A1 (senza sorvolare assembramenti di persone e presumibilmente neppure persone non coinvolte), non dovranno pesare più di 900 grammi (o non più di 250 se privi di marchio CE); per poter volare in categoria A2 (vicino a persone), non dovranno pesare più di 2 kg e dovranno mantenere almeno 50 m di distanza da persone non coinvolte. I droni fino a 25 kg potranno invece volare in categoria A3, dove dovranno essere condotti mantenendo una distanza di almeno 150 m da zone residenziali, industriali, ricreative e nella zona di volo non dovranno essere presenti persone non informate. Per tutte le *open categories*, ad eccezione di quelle realizzate con droni di peso inferiore ai 250 grammi, il pilota dovrà seguire un corso online superando un test svolto con la stessa modalità; per tutte le classi, ad esclusione dei droni rientranti nella categoria C0 e di quelli autocostruiti con peso inferiore a 250 g, dovrà essere applicato un dispositivo elettronico di identificazione; infine, per condurre tutti i droni dotati di dispositivo in grado di captare dati personali, come ad esempio una videocamera, sarà necessaria la previa registrazione, restando esonerati soltanto i droni di peso inferiore ai 250 g dichiarati giocattolo secondo la relativa direttiva europea.

---

[44] NPA 2017-05, spec. p. 5: "The EASA concept of UAS operations is highly inspired by the JARUS concept that identifies three categories, A, B, and C, related to the open, specific and certified category, respectively. The draft JARUS rules for category A and B are based on the EASA 'Prototype' Commission Regulation on Unmanned Aircraft Operations, published on 22 August 2016". Tale discrepanza è stata evidenziata anche nell'Opinion 1/2018, p. 7: " According to the concept defined in A-NPA 2015-10, UAS operations are classified into three categories:
— '"open" category' means a category of UAS operation that, considering the risks involved, requires neither a prior authorization by the competent authority, nor a declaration by the UAS operator before the operation takes place.
— '"specific" category' means a category of UAS operation that considering the risks involved, requires an authorization by the competent authority before the operation takes place, taking into account the mitigation measures identified in an operational risk assessment, except for certain standard scenarios for which a declaration by the UAS operator is sufficient, or when the operator holds a light UAS operator certificate (LUC) with the appropriate privileges.
— '"certified" category' means a category of UAS operation that, considering the risks involved, requires the certification of the UA and its operator, as well as licensing of the flight crew. This Opinion addresses UAS operations in the 'open' and 'specific' categories only (...)".

L'obbligo di registrazione degli operatori di un drone nei casi indicati già nel Regolamento n. 2018/1139, consistenti nelle ipotesi di utilizzo di (a) aeromobili senza equipaggio che, in caso di impatto, possono trasferire al corpo umano un'energia cinetica superiore a 80 joule; b) aeromobili senza equipaggio, il cui utilizzo comporta rischi per la riservatezza, la protezione dei dati personali, la *security* o l'ambiente; c) aeromobili senza equipaggio, la cui progettazione è soggetta a certificazione ai sensi dell'articolo 56, paragrafo 1[45]) è stato arricchito dalla previsione di cui all'art. 14 comma 5 del Reg. 2019/947, che prevede l'obbligo di immatricolazione anche per i droni aventi MTOM superiore a 250 g, e in tutte le ipotesi di operazioni specifiche.

Un ulteriore profilo normativo e definitorio interessante è quello relativo agli aeromodelli, considerati aeromobili senza equipaggio ai fini del regolamento droni, ed adoperati principalmente per lo svolgimento di attività ricreative. L'ENAC, nella versione originaria del Regolamento e fino all'ultima edizione aggiornata al 14 luglio 2020, li qualificava all'art. 5 come dispositivi impiegati esclusivamente per scopi ludici e sportivi, ed inoltre ne evidenziava la differenza rispetto ai SAPR (art. 1 comma 2), che per l'appunto "distingue(va), ai fini dell'applicazione delle disposizioni del Codice, i mezzi aerei a pilotaggio remoto in Sistemi Aeromobili a Pilotaggio Remoto (SAPR) e Aeromodelli", dettando per questi ultimi una disciplina specifica all'interno di un'apposita sezione del regolamento stesso.

Si dà atto che, coerentemente con la già citata assimilazione degli aeromodelli ai droni e all'avocazione delle competenze normative in capo all'EASA, la nuova versione del Regolamento ENAC del 4 gennaio 2021 non solo ha espunto la disciplina specificatamente riferibile a tali dispositivi - che aveva dato adito in dottrina a dubbi di legittimità[46] - ma ha eliminato anche la definizione di aeromodello, con ciò implicitamente aderendo all'unificazione classificatoria operata in ambito UE.

3. Droni, privacy e dati personali.

L'utilizzo e la diffusione dei droni costituisce indubbiamente una grande opportunità di crescita economica per tutti gli *stackeholders* del mercato unico europeo; di contro, il loro impiego su vasta scala potrebbe interferire con i diritti connessi alla tutela della privacy dei soggetti coinvolti[47].

[45] Allegato IX - Requisiti essenziali degli aeromobili senza equipaggio, punto 4, requisiti essenziali riguardanti la registrazione degli aeromobili senza equipaggio e dei loro operatori e la marcatura degli aeromobili senza equipaggio.

[46] F. Morello, Droni e assicurazioni aeronautiche. Spunti di diritto interno ed europeo, in Diritto dei Droni. Regole, questioni e prassi, pp. 223-241, spec. p. 235: "...il codice della navigazione, fonte primaria, assimila i SAPR agli aeromobili e ne demanda la disciplina ad una fonte secondaria (il Regolamento dell'Ente appunto), mentre nessun riferimento analogo si riscontra per gli aeromodelli, che ai sensi del codice della navigazione non sono aeromobili e per i quali manca una previsione di legge che legittimi la potestà regolamentare dell'ENAC in materia". V. anche E. G. Rosafio, Considerazioni sui mezzi aerei a pilotaggio remoto e sul regolamento ENAC, in Riv. dir. nav., 2014, 2, pp. 787-805.

[47] G. M. Riccio e F. Iraci Gambazza, Critical Infrastructures, use of drones and data protection impacts, in Diritto Mercato Tecnologia, 26 marzo 2020, pp. 1-26, spec. p. 10: "GDPR affected the drones regulation, from mainly four aspects: A) the broader meaning of personal data; the concept of accountability; B) the application of data protection by design or by default measures; C) all the rights granted to individuals, such

Dando uno sguardo preliminare alla normativa interna, i rilevamenti fatti tramite aerei sul territorio nazionale sono stati liberalizzati con il D.P.R. 29 settembre 2000, n. 367[48]. Ai fini dell'art. 2 del citato decreto, il rilevamento è "l'acquisizione di dati attraverso qualunque sensore"; dunque è lecito l'utilizzo delle comuni videocamere per riprese video amatoriali a fini prettamente personali. L'art. 3 comma 3 del medesimo decreto fa tuttavia salva "l'applicazione delle vigenti disposizioni in materia di trattamento dei dati personali relativamente ai dati raccolti nell'esercizio delle attività disciplinate dal regolamento".

Con specifico riguardo ai dispositivi aerei a pilotaggio remoto, l'art. 29 del nuovo Regolamento ENAC, rubricato "Protezione dei dati personali e privacy", dispone non solo che "laddove le operazioni svolte attraverso UAS possano comportare un trattamento di dati personali, tale circostanza deve essere menzionata nella documentazione sottoposta ai fini del rilascio della pertinente autorizzazione", ma anche e soprattutto che "il trattamento dei dati personali deve essere effettuato in ogni caso nel rispetto del Regolamento (UE) 2016/679 e del Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni (...)[49]".

In ambito UE, il Regolamento UE 2018/1139, al Considerando 28[50], richiama espressamente la necessità che le norme riguardanti gli aeromobili senza equipaggio contribuiscano al rispetto di quanto già previsto dalla normativa UE in materia di tutela della riservatezza e di protezione dei dati personali. La tutela degli stessi aspetti viene ribadita nell'Allegato IX del richiamato Regolamento, che individua quale requisito fondamentale dei droni quello di "possedere le relative caratteristiche e funzionalità specifiche che tengono conto dei principi della tutela della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita", al precipuo scopo di "attenuare i rischi inerenti alla sicurezza, alla tutela della vita riservatezza, alla protezione dei dati personali, alla security o all'ambiente derivanti dal loro esercizio".

---

as the right to be forgotten, the right to access data, etc.); D) the adoption of DPIA (data protection impact assessment) before using the technologies within the machines".
In argomento v. anche L. MERLA, Droni, privacy e tutela dei dati personali, in Inf. dir., 2016, p. 29 e segg., la quale offre anche degli spunti di comparazione tra la tutela della privacy negli Stati Uniti e in Europa; G. TADDEI ELMI, G. GIARDIELLO, F. ROMANO, Il dibattito sui droni: tra etica e privacy, in Diritto dei droni. Regole, questioni e prassi, a cura di E. Palmerini, M. A. Biasiotti, G. F. Aiello, cit., p. 35 e segg.

[48] Decreto del Presidente Della Repubblica, 29 settembre 2000, n. 367, Regolamento recante norme per la semplificazione dei procedimenti relativi a rilevamenti e riprese aeree sul territorio nazionale e sulle acque territoriali (n. 112-undecies dell'allegato 1 della legge n. 59/1997 e successive modificazioni). in GU, n.289 del 12-12-2000.

[49] In precedenza, l'art. 34 comma 2 dell'abrogato Regolamento Enac, nella terza ed ultima versione dell'11 novembre 2019, come emendata in data 14.7.2020, si limitava ad un generico rinvio a quanto previsto nel Codice in materia di protezione dei dati personali, nonché delle misure e degli accorgimenti a garanzia dell'interessato prescritti dal Garante per la protezione dei dati personali.

[50] Regolamento (UE) 2018/1139, Considerando 28: "Le norme riguardanti gli aeromobili senza equipaggio dovrebbero contribuire al rispetto dei diritti garantiti dal diritto dell'Unione, in particolare il rispetto della riservatezza e della vita familiare, sancito dall'articolo 7 della Carta dei diritti fondamentali dell'Unione europea, e la protezione dei dati di carattere personale, sancita dall'articolo 8 della Carta e dall'articolo 16 TFUE, e disciplinato dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio". Cfr. anche art. 132, comma 1: "Trattamento dei dati personali. 1. Per quanto riguarda il trattamento dei dati personali nel quadro del presente regolamento, gli Stati membri svolgono i loro compiti a norma del presente regolamento conformemente alle disposizioni legislative, regolamentari o amministrative nazionali in conformità del regolamento (UE) 2016/679".

Da quanto delineato si comprende che il panorama normativo italiano ed europeo è, allo stato, privo di una regolamentazione appositamente prevista per la sola attività dei droni, e si limita ad operare un generico e globale rinvio alla normativa generale - attualmente, dunque, al Regolamento *Privacy*[51] - stante l'assimilabilità delle problematiche afferenti a tale strumento a quelle relative ad altre tecnologie[52].

Di contro, ci sembra che ben possano emergere specifici profili di rischio riconducibili alle attività dei droni, connessi sia alla tutela della privacy che al trattamento dei dati personali[53]. In generale, l'impiego di questi strumenti sofisticati consente l'acquisizione di dati in forma dinamica e in modalità originali e più complesse rispetto a quelle sino ad oggi considerate: i droni sono in grado di raccogliere, produrre e sviluppare una grande quantità di dati di varia tipologia (immagini, dati biometrici, dati di spostamento, dati di comunicazione...) vista la loro maggiore libertà di movimento anche a bassa quota grazie alle dimensioni ridotte, e la presenza di tecnologie avanzate in grado di sopperire alla mancanza di un pilota fisico a bordo. Viene inoltre in rilievo, da un punto di vista marcatamente sociologico, il cd. *chilling effect* o effetto dissuasivo, derivante dall'aumento della sensazione di essere costantemente sottoposti a sorveglianza, con una possibile conseguente riduzione dell'esercizio di diritti e libertà civili[54], nonché il fenomeno del cd. uso

[51] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), G.U. 4.5.2016, L 119/1.
Per un commento alla nuova disciplina: V. CUFFARO, Il diritto europeo sul trattamento dei dati personali, in Contr. impr., 2018, p. 1098 ss; M. G. STANZIONE, Il regolamento europeo sulla privacy: origini e ambito di applicazione, in Eur. dir. priv., 2016, p. 1249; F. PIRAINO, Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato, in Nuove leggi civ. comm., 2017, p. 369; M. GRANIERI, Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679, ivi, p. 165; D. POLETTI, Il c.d. diritto alla disconnessione nel contesto dei «diritti digitali», in Resp. civ. prev., 2017, p. 8; I.A. CAGGIANO, Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale, in Annali dell'Università Suor Orsola Benincasa, 2018, p. 7 ss.; L. GATT, R. MONTANARI, I.A. CAGGIANO, Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali, in Pol. Dir., 2017, p. 343 ss.

[52] European Parliament, Directorate-General for internal policies, Privacy and Data protection implication in the civil use of drones. In-depth analysis for the LIBE Committee, 2015, p. 25: "...the European and Member States' regulatory frameworks are largely adequate to address the privacy, data protection and ethical impacts of RPAS due to their technological neutrality [...]".

[53] Il diritto alla privacy (o alla riservatezza) è normativamente distinto dal diritto alla protezione dei dati personali, anche se talvolta è difficile delinearne i confini in maniera netta. In generale, la protezione dei dati personali costituisce lo sviluppo della tutela della privacy (cd. right to be alone), allo scopo di estendere la tutela dell'individuo oltre la sfera della vita privata, assicurandone l'autodeterminazione decisionale e il controllo sulla circolazione dei propri dati. Se dunque tutelare la privacy si traduce nel divieto di compiere illegittime interferenze nella vita altrui, la tutela dei dati personali assicura il costante controllo da parte del titolare dei dati in ogni operazione di acquisizione e trattamento dei medesimi. Cfr. in dottrina G. RESTA, Il diritto alla protezione dei dati personali, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), Il codice dei dati personali: temi e problemi, Milano, 2004, p. 19 ss; A. M. GAMBINO e A. STAZI (a cura di), La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele, Pisa, 2020; A. ADDANTE, L'accesso ai dati personali quale corrispettivo di contenuti e servizi digitali, in AA.VV., La circolazione della ricchezza nell'era digitale (Atti della Summer School 2020), Pisa, 2021, p. 397 e segg.; D. FARACE, Le persone autorizzate al trattamento dei dati personali, in Riv. trim. dir. proc. civ., 2021, p. 423 e segg.

[54] Sulla sindrome dell'effetto dissuasivo e dell'effetto panottico, dovuta a un uso su larga scala dei droni, cfr. lo studio di R. L. FINN, D. WRIGHT e A. DONOVAN (Trilateral Research & Consulting, LLP), L. JACQUES e P. DE HERT (Vrije Universiteit Brussel), "Privacy, data protection and ethical risks in civil RPAS operations" [Tutela della

distorto dei droni (cd. *function creep*), volto all'impiego degli stessi per uno scopo diverso da quello originariamente previsto.

I problemi si pongono sia a monte, in relazione al rispetto degli obblighi di trasparenza e correttezza (tra cui va annoverata la necessaria acquisizione del consenso informato), sia a valle, circa il regime di responsabilità degli utilizzatori dei droni nelle ipotesi di violazione della normativa.

In generale, i SAPR sono dotati di *visual recording equipments* con capacità di riconoscimento facciale a bordo o da terra, che permettono di identificare e tracciare specifici individui[55]; ciò determina che i dati trattati dai SAPR possono essere sia personali che sensibili, intendendosi, nel primo caso, qualsiasi informazione riguardante un soggetto, identificato o identificabile (direttamente o indirettamente) per mezzo di un nome, di un numero di identificazione, di dati relativi all'ubicazione, di un identificativo online o di uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 n. 1 del GDPR) e, nel secondo, tutte quelle informazioni che, all'interno della prima categoria, possono rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art .9 comma 1 del GDPR).

Con riguardo ai dati personali non sensibili, la principale condizione di liceità del trattamento degli stessi si basa sul consenso dell'interessato (art. 6 comma 1 lett. a) del GDPR); in molti casi tuttavia, stante la materiale difficoltà di richiedere ed ottenere il predetto consenso da tutti i soggetti effettivamente coinvolti, dovrà farsi riferimento ad una diversa base legale, ad esempio il perseguimento del legittimo interesse del titolare del trattamento, tenuto conto - alla luce del Considerando 47 del GDPR - anche delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Per esempio, tali interessi potrebbero sussistere nell'ipotesi in cui intercorra una "relazione pertinente ed appropriata tra l'interessato e il titolare del trattamento", purché sia costantemente monitorata l'eventualità che l'interessato "possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine".

Pertanto, come è stato chiarito anche dall'art. 29 Working Party[56], gli elementi in base ai quali dovrà valutarsi l'eventuale prevalenza del legittimo interesse in capo al titolare sono: le modalità di utilizzo dei dati; le aspettative in punto di *an* e *quantum* del trattamento degli stessi; la relazione intercorrente tra titolare del trattamento e soggetti interessati; gli strumenti specifici a tutela del trattamento dati e la loro qualità. Ulteriori problemi possono sorgere dal trattamento dei cd. dati di ubicazione e di movimento: essi sono esplicitamente considerati un identificativo, che rende *ex se* individuabile

vita privata, protezione dei dati e rischi etici nelle operazioni civili degli RPAS], del 7 novembre 2014, disponibile sul sito: http://ec.europa.eu/DocsRoom/documents/7662, pag. 28 e seguenti

[55] Trattasi di telecamere intelligenti con lunghezza focale fissa o variabile, in grado di memorizzare e trasmettere immagini in diretta, con capacità di riconoscimento facciale a bordo o con base a terra, che permettono ai droni di identificare e seguire specifici individui, Article 29 parere, p. 7

[56] Cfr. altresì il parere 06/2014 del gruppo di lavoro Articolo 29 per la protezione dei dati sul concetto di interesse legittimo del responsabile del trattamento, WP217, pag. 20 e 21.

qualsiasi soggetto ad essi associato[57]. Non esistono infatti dati di ubicazione anonimi o non personali, perché ogni volta che in un punto dello spazio viene identificata la presenza di una persona fisica, qualsiasi informazione o dato costituirà di per sé un'ipotesi di trattamento di dati personali.

Inoltre, il Regolamento di esecuzione 947/2019 impone uno specifico obbligo di immatricolazione per i droni in grado di raccogliere dati personali, salvo il caso di aeromobile considerato giocattolo ai sensi della direttiva 2009/48/CE[58].

Nel caso in cui il SAPR faccia uso di dati sensibili, sono necessarie ulteriori garanzie, *in primis* l'ottenimento del consenso "esplicito" del soggetto interessato, ovvero la presenza di un altro caso di esclusione del divieto di trattamento di categorie particolari di dati, come ad esempio la circostanza che i predetti dati sensibili siano stati resi manifestamente pubblici dall'interessato (art. 9 comma 2 lett. e)[59] del GDPR).

È inoltre opportuno evidenziare che l'acquisizione di dati da parte dei privati effettuato con l'uso di droni per operazioni civili potrebbe non essere sottoposta alle disposizioni del Regolamento privacy, ad esempio nel caso di esercizio di attività a carattere esclusivamente personale o domestico (cd. *household exception*), di cui all'art. 2 comma 2 lett. c)[60] del GDPR. La predetta eccezione, come stabilito dalla Corte di giustizia dell'Unione europea, va interpretata in modo restrittivo, non trovando applicazione né laddove i dati siano successivamente diffusi tramite Internet o altro mezzo di divulgazione[61], né quando la raccolta degli stessi, pur rivestendo carattere personale, sia stata eseguita in spazi pubblici[62].

---

[57] Art. 4, n. 1) GDPR: "(...) si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a (...) dati relativi all'ubicazione (...)".

[58] Considerando 19: "In considerazione dei rischi per la riservatezza e la protezione dei dati personali, gli operatori di aeromobili senza equipaggio dovrebbero essere immatricolati se utilizzano aeromobili senza equipaggio dotati di sensori in grado di raccogliere dati personali. Tuttavia, ciò non dovrebbe avvenire quando l'aeromobile senza equipaggio è considerato un giocattolo ai sensi della direttiva 2009/48/CE del Parlamento europeo e del Consiglio sulla sicurezza dei giocattoli"; art. 14 comma 5: " 5. Gli operatori UAS sono tenuti a immatricolarsi: a) quando operano nell'ambito della categoria «aperta» utilizzando uno dei seguenti aeromobili senza equipaggio: [...] ii. aeromobili senza equipaggio dotati di un sensore in grado di rilevare dati personali, a meno che non sia conforme alla direttiva 2009/48/CE".

[59] G. MALGIERI, La titolarità dei dati trattati per mezzo dei droni tra privacy e libertà intellettuale, in Diritto dei droni. Regole, questioni e prassi, cit., pp. 163-197, spec. p. 189 problematicamente si chiede "se lo sfoggiare in pubblico (nel raggio visuale di un SAPR appunto) l'appartenenza ad una razza o etnia, l'aderenza ad un partito, ad un sindacato o ad una religione o un proprio stato di salute possa ritenersi un "rendere manifestamente pubblico" da parte dell'interessato determinati dati sensibili". La risposta fornita prevede un triplice ordine di ipotesi: è affermativa, se la manifestazione costituisce espressione di una scelta consapevole del soggetto (ad esempio, la partecipazione ad un corteo); è negativa, se emerge dal solo fatto di trovarsi in pubblico; dipende dalle circostanze del caso concreto (approccio casistico) nel caso di attività intermedie o necessarie per lo svolgimento della vita associativa.

[60] Reg. (UE) 2016/679, Articolo 2, Ambito di applicazione materiale: 2. Il presente regolamento non si applica ai trattamenti di dati personali: (...) c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico".

[61] Corte di giustizia dell'Unione europea, sentenza nella causa C-101/01, Bodil Lindqvist case, 6 novembre 2003, punto 47, in cui si statuisce che l'esenzione per le attività domestiche deve "interpretarsi nel senso che comprende unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone".

[62] Corte di giustizia dell'Unione europea, sentenza nella causa C-212/13, František Ryneš contro Úřad pro ochranu osobních údajů, 11 dicembre 2014, punto 33 : se la registrazione e la conservazione dei dati si estende "anche se solo parzialmente, allo spazio pubblico, e pertanto è diretta verso l'esterno della sfera privata della persona che procede al trattamento dei dati con tale modalità, essa non può essere considerata

Un secondo ambito di deroghe potrebbe riguardare l'attività di acquisizione di dati per finalità giornalistiche, artistiche o di espressione letteraria (indipendentemente dal perseguimento di uno scopo di lucro[63]): sul punto, in linea con l'art. 9[64] dell'abrogata Direttiva 95/46/CE[65], l'art. 85 comma 2 del GDPR lascia agli Stati membri la possibilità di prevedere esenzioni o deroghe, limitatamente ai casi in cui siano "necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione[66]".

Un ulteriore profilo problematico attiene all'individuazione del responsabile e del titolare del trattamento dei dati impiegati o raccolti dal SAPR, come definiti rispettivamente dall'art. 4, numeri 7) e 8)[67] del GDPR, individuazione non sempre agevole vista la possibilità di controllo del mezzo da remoto o tramite software automatici da parte dell'operatore del drone. In generale, il titolare del trattamento dati (*controller*) è colui che ne determina le finalità e i mezzi, mentre il responsabile del trattamento (*processor*) è colui che tratta di tali dati per conto del titolare; nella pratica, tali attività sono di frequente svolte da soggetti diversi[68] e ben potrebbero costituire espressione ed attuazione di un progetto condiviso[69]. In tale specifica ipotesi, verrebbe in rilievo la figura del contitolare del trattamento, espressamente prevista dall'art. 26[70] del GDPR,

un'attività esclusivamente «personale o domestica» ai sensi dell'articolo 3, paragrafo 2, secondo trattino, della direttiva 95/46".

[63] Un'attività può essere qualificata come "attività giornalistica" qualora sia diretta a "divulgare al pubblico informazioni, opinioni o idee, indipendentemente dal mezzo di trasmissione utilizzato. Esse non sono riservate alle imprese operanti nel settore dei media e possono essere connesse a uno scopo di lucro." (Corte di giustizia dell'Unione europea, sentenza nella causa C-73/07, Tietosuojavaltuutettu contro Satakunnan Markkinapörssi Oy e Satamedia Oy, 16 dicembre 2008, punto 61).

[64] Direttiva 95/46/CE, Articolo 9, Trattamento di dati personali e libertà d'espressione: Gli Stati membri prevedono, per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria, le esenzioni o le deroghe alle disposizioni del presente capo e dei capi IV e VI solo qualora si rivelino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione.

[65] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, G.U. n. L 281 del 23.11.1995.

[66] Reg. (UE) 2016/679, Articolo 85, Trattamento e libertà d'espressione e di informazione: 1. Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria. 2. Ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedono esenzioni o deroghe rispetto ai capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione.

[67] Reg. (UE) 2016/679, Articolo 4, Definizioni: (...): 7) "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74) 8) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

[68] G. MALGIERI, La titolarità dei dati trattati per mezzo dei droni tra privacy e libertà intellettuale, cit., spec. p. 173, in cui si riporta il seguente esempio relativo al settore della fotografia professionale: "un committente (cliente privato) stabilisce le finalità; il professionista (fotografo) stabilisce le modalità; potrebbe esserci un soggetto diverso a controllare il drone (il pilota remoto), il quale concorre a stabilire gli strumenti utilizzati".

[69] Si veda il documento Article 29 Data Protection Working Party, Opinion n. 1/2010 on the concepts of "controller" and "processor", 00264/EN, WP 169, adopted on 16 febbraio 2010.

[70] Reg. (UE) 2016/679, Articolo 26, Contitolari del trattamento: 1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi

che richiede a ciascuno di essi la stipula di un accordo interno di ripartizione delle responsabilità circa gli obblighi derivanti dal trattamento dati.

L'abrogato Regolamento ENAC conteneva una previsione analoga nell'art. 7 comma 3, il quale disponeva che "nel caso di operazioni specializzate per conto terzi, deve essere stipulato un accordo tra l'operatore del SAPR e il committente nel quale le parti definiscono le rispettive responsabilità per la specifica operazione di volo e sulle eventuali limitazioni e condizioni connesse, anche con riguardo alle disposizioni in materia di protezione dati (...)". Tale regola, pur non essendo stata riproposta né nei regolamenti nn. 945 e 947 della Commissione, né nel nuovo Regolamento ENAC del 2021, troverà comunque applicazione in forza del solo art. 26 del GDPR, in quanto normativa di generale applicazione a tutte le fattispecie di *joint-controllership*.

È di fondamentale importanza chiarire che l'impiego dei SAPR in relazione alla tutela della privacy richiede l'approfondimento del concetto di *Privacy Enhancing Tehnologies*[71], ossia delle tecnologie utili ad implementare la protezione dei dati personali, poi sviluppatosi nella *Privacy by Design*. Dapprima teorizzata da Ann Cavoukian nel 2009, poi formalizzata come *global privacy standard* durante la *32nd International Conference of Data Protection and Privacy Commissioners* svolta nel 2010 a Gerusalemme, è stata da ultimo codificata nell'art. 25 del GDPR[72], rubricato "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita": l'articolo in esame dispone che il titolare del trattamento debba mettere in atto misure tecniche

---

determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati. 2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato. 3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento".

[71] Già a metà degli anni '90, a seguito di uno studio svolto dalla Dutch Registratierkamer (ora "College Bescherming Persoonsgegevens") in collaborazione con l'Information and Privacy Commissioner of Ontario, fu redatto un documento dal titolo "Privacy Enhancing Technologies: the path to anonymity" in cui comparve per la prima volta l'espressione Privacy Enhancing Technologies152 (PET) per indicare l'insieme di tutti gli strumenti, non particolarmente invasivi, che in ambito ICT sono utili per modellare i sistemi informativi al fine di accrescere la protezione e la sicurezza dei dati personali. Per approfondimento si veda Information and Privacy Commissioner of Ontario, Dutch Registratierkamer, Privacy Enhancing Technologies - The Path to Anonymity, Registratiekamer, The Netherlands, Voll. I-II, 1995; D. MARTIN, A. SERJANTOV (edited by), Privacy Enhancing Technologies, Proceeding of 4° international workshop, PET 2004, Toronto, May 2004, Berlin. In particolare i principi chiave su cui si basano le PET sono essenzialmente: a) la minimizzazione della raccolta, dell'utilizzo, della divulgazione e della conservazione dei dati identificativi degli utenti; b) la partecipazione e il coinvolgimento attivo degli utenti, tra l'altro, permettendo l'esercizio di poteri di controllo durante il ciclo di vita dei dati personali trattati; c) la maggiore sicurezza delle informazioni sensibili, sia sotto il profilo del diritto alla riservatezza sia sotto il profilo dell'integrità dei dati, ottenuta attraverso tecniche di anonimizzazione e di deidentificazione delle informazioni sensibili.

[72] Al fine di chiarire questi i concetti espressi nell'articolo 25 occorre guardare il Considerando 78 del GDPR in cui si legge "La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. […] In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati".

e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento stesso e tutelare i diritti degli interessati; ciò, anche tramite misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento.

Anche nello specifico ambito nei SAPR si ritiene opportuno valorizzare tecniche riconducibili ai principi della *privacy by design e by default* per incorporare, fin dalla progettazione del drone, soluzioni rispettose della normativa sulla privacy, senza che all'utilizzatore del drone sia richiesto il compimento di un'attività ulteriore di monitoraggio o di gestione dello strumento. Si pensi, ad esempio, alla possibile installazione di un software direttamente nel dispositivo di videoripresa, in grado di riconoscere automaticamente i volti umani e di procedere automaticamente alla cancellazione dei fotogrammi o ad un oscuramento o sfocatura del volto; ovvero all'introduzione di una impostazione per la cancellazione automatica dei fotogrammi trascorso un determinato intervallo di tempo dalla loro registrazione.

Il rispetto del principio della *privacy by design* determina altresì un cambio di approccio, da intendersi non solo come reattivo e rimediale (si pensi al *data breach*) ma anche e prima di tutto proattivo, con riguardo ai vincoli imposti dal *Privacy Impact Assessment* (PIA), di cui all'art. 35 del GDPR e più ampiamente dall'*accountability*. In particolare, si potrebbe prevedere una valutazione d'impatto per i produttori per i droni "progettati e prodotti" ai fini di sorveglianza e per gli operatori che usano droni con apparecchi "audiovisivi" a bordo. Con specifico riguardo alle operazioni UAS rientranti nella "categoria specifica", il Reg. 2019/947 richiede all'operatore l'espletamento di tutte le procedure idonee a rispettare la normativa di cui al GDPR ed inoltre, laddove sia richiesto dall'autorità nazionale per la protezione dati, di compiere la valutazione d'impatto di cui all'art. 35[73].

[73] Allegato Operazioni UAS nelle categorie "Aperta e specifica", Parte B Operazioni UAS nella categoria specifica, UAS.SPEC.050 Responsabilità dell'operatore UAS: "1) L'operatore UAS deve soddisfare tutte le seguenti condizioni: a) stabilire procedure e limitazioni adeguate al tipo di operazione previsto e al rischio connesso, tra cui: [...] iv. procedure volte a garantire che tutte le operazioni rispettino il regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. In particolare, deve effettuare una valutazione d'impatto sulla protezione dei dati, se richiesto dall'autorità nazionale per la protezione dei dati in applicazione dell'articolo 35 del regolamento (UE) 2016/679.

Conclusioni.

Nella dialettica tra tecnologia e diritto, ogni riflessione giuridica su di un fenomeno particolarmente innovativo è in grado di generare problematiche simili, in relazione all'opportunità di agire a livello normativo e circa le migliori modalità di realizzazione di tale intervento[74].

In caso di mancanza di norme specifiche volte a disciplinare il nuovo fenomeno, si sottolinea l'esigenza di un intervento legislativo urgente, al fine di colmare la lacuna del sistema, per garantire sicurezza agli operatori del settore, senza scoraggiare le possibilità di crescita economica e tecnologica del mercato. Proprio in risposta a tali istanze, il legislatore europeo è intervenuto di recente a regolamentare la materia, sia pure con riguardo alla sola disciplina dell'uso dei droni.

Più in generale, la regolazione dello strumento del drone è caratterizzata, da un lato, dal perseguimento di *standards* comuni di sicurezza, connessi a specifici processi di certificazione della conformità, soprattutto alla luce del Regolamento delegato n. 947/2019[75]; dall'altro, dal costante impiego della cd. tecno-regolazione (o regolazione non normativa), che richiede l'inserimento di strumenti tecnici nel sistema operativo, per consentire il rispetto delle regole giuridiche, in un'ottica di parziale esternalizzazione della riposta giuridica, delegata alla normazione tecnica, come già avvenuto in sede di GDPR, grazie all'espresso richiamo in esso contenuto del concetto di *privacy by design*.

In altri termini, nel contesto normativo attuale, risulta sempre più diffusa la creazione e la diffusione di "regole tecniche" che delineano in maniera chiara le caratteristiche strutturali e gli *standards* di sicurezza dei mezzi aerei a

[74] Per l'analisi del rapporto tra diritto e nuove tecnologie, sia consentito il rinvio a E. Palmerini, The interplay between law and technology, or the RoboLaw project in context, in E. Palmerini, E. Stradella (a cura di), Law and Technology. The Challenge of regulating technological development, Pisa, 2013, p. 7 ss; G. Finocchiaro, Riflessioni su diritto e tecnica, in Il Diritto dell'informazione e dell'informatica, 2012, 4-5, pp. 831-840, spec. p. 840: "Come il giurista non deve inventarsi tecnologo, benché debba comprendere a fondo la tecnologia, analogamente al tecnico non spetta la scelta dei valori né´ l'interpretazione del diritto. Il dialogo è essenziale, la comprensione reciproca anche, ma nel rispetto dei rispettivi ruoli. È importante ristabilire rispetto e confini, rivendicando con orgoglio il ruolo del giurista". Sul punto, si vedano altresì le considerazioni di P. Stanzione: "L'avvento delle nuove tecnologie ha segnato una vera e propria rivoluzione antropologica, ma altresì sociale, culturale, politica, economica. Come rispetto a ogni fenomeno "disruptive", il rischio da evitare è quello di un'eterna rincorsa, da parte del diritto, di una tecnica quasi irraggiungibile per velocità e profondità dell'evoluzione.
La chiave per il governo dell'innovazione appare invece, da un lato, quella della duttilità e lungimiranza garantite dal principio di neutralità tecnologica, dall'altro, quella dell'approccio antropocentrico alla tecnica", come espresse nella prefazione al volume La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele, cit.

[75] Specificamente, v. Considerando 6: "Gli UAS che non sono considerati giocattoli a norma della direttiva 2009/48/CE dovrebbero essere conformi ai pertinenti requisiti essenziali di sicurezza e di tutela della salute di cui alla direttiva 2006/42/CE del Parlamento europeo e del Consiglio, nella misura in cui tale direttiva sia ad essi applicabile, sempre che tali requisiti di sicurezza e di tutela della salute non siano intrinsecamente legati alla sicurezza di volo degli UAS: Nei casi in cui detti requisiti di sicurezza e di tutela della salute sono intrinsecamente legati alla sicurezza di volo si applica solo il presente regolamento"; Articolo 6 - obblighi dei fabbricanti: "1. All'atto di immissione del loro prodotto sul mercato, i fabbricanti assicurano che il prodotto sia stato progettato e fabbricato conformemente ai requisiti di cui alle parti da 1 a 6 dell'allegato. 2. (...) Qualora la conformità del prodotto ai requisiti di cui alle parti da 1 a 6 dell'allegato sia stata dimostrata da tale procedura di valutazione della conformità, i fabbricanti redigono una dichiarazione di conformità UE e appongono la marcatura CE".

pilotaggio remoto [76]. La giuridicizzazione di questi parametri tecnici - da realizzare previo richiamo degli stessi attraverso le fonti di normazione primaria - può risultare di grande utilità al fine di garantire l'efficace funzionamento del mercato ed una sana competizione tra gli operatori del settore nell'Unione europea[77].

[76] Coglie esattamente il punto (ancorché in un saggio avente argomento diverso) E. AL MUREDEN, Product safety e product liability nella prospettiva del danno da prodotto conforme, in G. ALPA (a cura di), La responsabilità del produttore, Milano, 2019, pp. 489-521, spec. p. 495.

[77] Reg. UE 1139/2018, Articolo 1, Oggetto e finalità: "(...) 2. Il presente regolamento intende inoltre: (...) b) facilitare, nei settori disciplinati dal presente regolamento, la libera circolazione delle merci, delle persone, dei servizi e dei capitali, offrendo parità di condizioni per tutti gli operatori nel mercato interno dell'aviazione, e migliorare la competitività dell'industria aeronautica dell'Unione".

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Campioni biologici da vivente capace e biobanche di ricerca: raccolta, utilizzo e circolazione.

Capable living biological samples and research biobanks: collection, use and circulation.

GIANLUCA MONTANARI VERGALLO
Professore associato di Medicina legale
Università di Roma "Sapienza"

Abstract

L'articolo esamina la disciplina italiana e dell'Unione europea in materia di biobanche di ricerca, concentrandosi su raccolta, utilizzo e circolazione dei campioni da vivente capace, nella prospettiva del bilanciamento tra diritti alla privacy, all'identità e all'autodeterminazione, da un lato, e interesse pubblico alla ricerca scientifica, dall'altro. Dall'insieme dei principi e delle disposizioni emerge che la soluzione più aderente al dato positivo e più idonea a contemperare gli indicati interessi contrapposti non è l'anonimizzazione del campione, ma l'adozione del modello di consenso multi-opzione. Inoltre, il consenso non attribuisce alla biobanca un diritto reale. Di conseguenza, la biobanca può trasferire il materiale biologico solo nei limiti del consenso dell'originario concedente.

The article is meant to lay out an analysis of Italian and EU legislative and regulatory frameworks governing biobanks that store biological samples (usually human) for research purposes, by focusing closely on collection, use and sharing of samples from living individuals, as well as on the possible balance between the rights to privacy, personal identity, self-determination and the public interest in advancing scientific research. From an overview of all sets of principles and regulations, it may be argued that the best solution, in terms of positive outcomes and reconciling the above mentioned opposing interests, is not the anonymization of samples, but rather the introduction of multi-optional consent. Such consent does not ascribe absolute ownership to biobanks. Consequently, biobanks can only share and transfer biological materials within the limitations originally outlined and agreed to by the consenting individual.

Parole chiave: campioni biologici; biobanche di ricerca; sperimentazione; privacy; autodeterminazione; identità personale

Keywords: biological samples; research biobanks; experimentation; privacy; self-determination; personal identity.

Summary: Introduzione: la funzione delle biobanche di ricerca. – 1. La tutela della riservatezza. – 2. La tutela del diritto all'identità e all'autodeterminazione. – 3. Raccolta e utilizzo del materiale biologico. – 4. Circolazione del materiale biologico. – Conclusioni.

Introduzione: la funzione delle biobanche di ricerca.

In Europa la disciplina delle biobanche è prevalentemente rimessa ai legislatori nazionali, essendosi limitata l'Unione ad adottare direttive e due raccomandazioni, prima nel 2004 e, da ultimo, nel 2016. La direttiva 2004/23 [1] usa la locuzione «istituto di tessuti», inteso come «una banca dei tessuti o un'unità di un ospedale o un altro organismo in cui si effettuano attività di lavorazione, conservazione, stoccaggio o distribuzione di tessuti e cellule umani. L'istituto dei tessuti può inoltre essere incaricato dell'approvvigionamento o del controllo dei tessuti e delle cellule» [2]. Si tratta, dunque, di una collezione di materiale biologico umano [3]. Quest'ultimo include tutto ciò che proviene dal corpo umano ed è composto da cellule umane, quindi

[1] Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:102:0048:0058:en:PDF. Tale direttiva è stata attuata dapprima dalle direttive 2006/17/CE e 2006/86/CE per quanto riguarda le prescrizioni tecniche per la donazione, l'approvvigionamento e il controllo di tessuti e cellule umani, nonché per quanto riguarda le prescrizioni in tema di rintracciabilità, la notifica di reazioni ed eventi avversi gravi e determinate prescrizioni tecniche per la codifica, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani», a loro volta attuate dal D.Lgs. 25 gennaio 2010, n. 16, e successivamente dalla direttiva 8 aprile 2015, n. 2015/566, «per quanto riguarda le procedure volte a verificare il rispetto delle norme di qualità e di sicurezza equivalenti dei tessuti e delle cellule importati», pubblicata nella G.U.U.E. 9 aprile 2015, n. L 93 ed entrata in vigore il 29 aprile 2015, attuata dall'Italia con il D.Lgs. 16 dicembre 2016, n. 256.

[2] Nell'attuare tale direttiva, l'Italia ha precisato che i compiti dell'Istituto di tessuti possono comprendere «anche l'esecuzione degli esami analitici» (art. 3 D.Lgs. 6 novembre 2007, n. 191).

[3] In tal senso, l'art. 2, lett. a) del decreto del Ministero delle Attività Produttive del 26 giugno 2006 adotta come definizione quella di «centri fornitori di servizi per la conservazione, il controllo e l'analisi di cellule viventi, di genomi di organismi e informazioni relative all'ereditarietà e alle funzioni dei sistemi biologici, i quali conservano organismi coltivabili (microrganismi, cellule vegetali, animali e umane), parti replicabili di essi (genomi, plasmidi, virus, DNA), organismi vitali ma non più coltivabili, cellule e tessuti, così come anche banche dati concernenti informazioni molecolari, fisiologiche e strutturali rilevanti per quelle collezioni». Analogamente, anche il parere del Comitato nazionale per la bioetica, *Biobanche pediatriche*, dell'11 aprile 2014, qualifica le biobanche come «unità operative e di servizio, preposte a raccogliere, conservare, classificare, gestire e distribuire materiali biologici umani (cellule, tessuti, DNA) d'individui o gruppi d'individui sani o malati, per finalità biomediche (di ricerca, di diagnosi, di prevenzione o di terapia), all'interno dei presidi ospedalieri o centri di ricerca»; il parere è consultabile al sito http://bioetica.governo.it/media/1821/p116_2014_biobanche_pediatriche_it.pdf. Analoga, ma meno dettagliata, la definizione contenuta nel parere del Comitato nazionale per la biosicurezza e le biotecnologie, *Linee guida per la certificazione delle biobanche*, 19 aprile 2006, consultabile al sito http://cnbbsv.palazzochigi.it/media/1629/2006-19-aprile-biobanche_1.pdf.

non solo organi e tessuti, ma anche la saliva, ad esempio [4].

La collezione di tali campioni, insieme alle associate informazioni cliniche sui pazienti, rappresenta un supporto scientifico fondamentale per la medicina personalizzata [5], detta anche medicina di precisione o individualizzata perché propone misure diagnostiche, preventive e terapeutiche commisurate al singolo paziente alla luce delle informazioni sul suo corredo biologico, al fine di una maggior efficacia del trattamento e della riduzione degli effetti collaterali [6]. L'identificazione di biomarcatori che sono specificamente associati a particolari condizioni mediche come cancro, malattie cardiovascolari e disturbi neurologici è utile per la diagnosi precoce, la prevenzione e il trattamento delle malattie. La capacità di determinare singoli biomarcatori tumorali e di utilizzarli per la diagnosi della malattia, la prognosi e la previsione della risposta alla terapia sta avendo un impatto molto significativo sulla medicina personalizzata e sta cambiando rapidamente il modo in cui viene condotta l'assistenza clinica. Poiché un requisito fondamentale per la medicina personalizzata è la disponibilità di un'ampia raccolta di campioni di pazienti con dati clinici e patologici del paziente ben annotati, le biobanche svolgono un ruolo importante nel progresso della medicina personalizzata [7].

Il preambolo alla raccomandazione del Consiglio d'Europa dell'11 maggio 2016, in materia di ricerca su materiale biologico di origine umana, riconosce che le collezioni di materiale biologico presentano un notevole potenziale di miglioramento dell'assistenza e della qualità di vita delle persone attraverso il loro uso nella ricerca biomedica [8].

Tuttavia, poiché dal materiale biologico è possibile estrarre informazioni genetiche e sulla salute della persona da cui proviene, l'uso di tale materiale può comportare una violazione della riservatezza, tanto più evidente in caso di dati genetici, perché coinvolgono anche i familiari della persona da cui è prelevato il campione [9]. Dunque, sia il legislatore che l'interprete devono tendere alla ricerca del miglior bilanciamento tra diritti individuali ed interesse

---

[4] In Italia, come rileva D. Farace, *Campioni biologici*, in *Enc. giur.*, agg. 2017, vol. I, p. 1, la circolare del ministero della Salute 8 maggio 2003, n. 3, recante «Raccomandazioni per la sicurezza del trasporto di materiali infettivi e di campioni diagnostici», definisce campioni diagnostici «tutti i materiali di origine umana o animale, inclusi escreti, sangue e suoi componenti, tessuti e fluidi tessutali, raccolti a scopo diagnostico».

[5] A. Liu, K. Pollard, *Biobanking for personalized medicine*, in F. Karimi Busheri (a cura di), *Biobanking in the 21st century*, Springer International Publishing, 2015, 55-68. Per ampie considerazioni sulle funzioni delle biobanche di ricerca si rinvia a Comitato nazionale per la biosicurezza e le biotecnologie, *Linee guida per la certificazione delle biobanche*, 19 aprile 2006, cit.

[6] F.R. Vogenberg, C.I. Barash, M. Pursel, *Personalized Medicine Part 1: Evolution and Development into Theranostics*, in *Pharmacy and Therapeutics*, 2010, 35(10), 560-562, 565-567, 576.

[7] A. Liu, K. Pollard, *Biobanking for personalized medicine*, cit.

[8] Su questa base, J. StjernschantzForsberg, M.G. Hansson, Eriksson, *Biobank Research: Who Benefits from Individual Consent?*, in *BMJ* 2011, 343, d5647, sostengono che l'acquisizione del consenso alla raccolta e al trattamento dei campioni biologici sarebbe superfluo, perché tali condotte sarebbero giustificate dallo scopo scientifico della ricerca, che potrebbe portare ad un miglioramento della salute delle future generazioni e persino dello stesso donatore. Nei successivi paragrafi saranno evidenziati i numerosi dati normativi che rendono non condivisibile questa tesi.

[9] Infatti, nel parere del 5 giugno 2019, il Garante della privacy prevede al punto 4.11, per il trattamento di dati genetici per finalità di ricerca scientifica, regole più restrittive di quelle contenute al punto 5 relativamente al trattamento di dati personali effettuato per i medesimi scopi (Garante della privacy, Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 del 5 giugno 2019, in G.U. n. 176 del 29 luglio 2019, consultabile anche all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9124510).

pubblico alla ricerca biomedica.

1. La tutela della riservatezza.

Il tema oggetto del presente contributo rientra nell'ambito di applicazione del Regolamento europeo sulla privacy, recepito dall'Italia con il D.Lgs. 10 agosto 2018, n. 101, che ha modificato il codice della privacy del 2003. Le ampie definizioni di «dato personale» e di «trattamento», accolte dal legislatore europeo, appunto includono la «raccolta», l'«uso» e la «messa a disposizione» di «qualsiasi informazione riguardante una persona fisica identificata o identificabile» (art. 4, nn. 1 e 2). Anche la nozione di «dati genetici», di cui al n. 13 dell'art. 4, riguardando conoscenze non solo sulle caratteristiche genetiche ereditarie che influiscono sulla salute di una persona fisica, ma anche quelle sulle caratteristiche genetiche acquisite che «forniscono informazioni univoche sulla fisiologia» di tale individuo, è abbastanza inclusiva da riferirsi a tutto il "sapere" che può essere ricavato dai campioni biologici contenuti nelle biobanche.

Ai sensi degli artt. 6 e 9 del Regolamento europeo, il trattamento sia dei dati personali "non qualificati" sia di quelli genetici o relativi alla salute deve avvenire con l'esplicito consenso dell'interessato [10] e per specifiche finalità [11]. Tuttavia, si può prescindere dal consenso in numerose ipotesi, la cui disciplina talora è differente per le «particolari categorie di dati» di cui all'art. 9. Di conseguenza, poiché l'attività di ricerca comporta l'acquisizione di dati attinenti alla salute e talora anche genetici [12], per le condizioni di liceità del trattamento senza consenso occorre fare riferimento proprio a quest'ultima disposizione. L'ipotesi più pertinente è riportata alla lett. j) dell'art. 9, ossia quella del trattamento «necessario a fini di archiviazione nel pubblico interesse, di ricerca

[10] Come rileva I.A. Caggiano, *Il consenso al trattamento dei dati personali tra nuovo Regolamento Europeo e analisi comportamentale*, in https://www.unisob.na.it/ateneo/annali/2016-2018_1_Caggiano.pdf, p. 20, l'uso del termine «esplicito», in luogo di «espresso», denota che il consenso non sia desumibile da comportamenti concludenti, sebbene il Regolamento europeo non preveda il requisito di forma *ad substantiam* né autorizzazione del Garante, che invece erano stati introdotti dal legislatore nazionale all'art. 26. Si veda altresì I.A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Osservatorio dir civ comm.*, 2018, 1, 67-106.

[11] L. Gatt, R. Montanari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, 2017, II, 337 ss. Come rileva G. Comandé, *Ricerca in sanità e* data protection *un* puzzle *… risolvibile*, in *Riv. it. med. leg. dir. san.*, 2019, 189, parag. 3, «Proprio questo requisito generale è problematico per la ricerca *data-intensive* e per il riuso. Il problema non è rimasto inascoltato dal legislatore europeo che al considerando 33 apre la strada a forme di consenso ampio affermando: "In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista."».

[12] Come rilevano C. Ricci, P. Ricci, *Le biobanche di ricerca: questioni e disciplina*, in *Riv. it. med leg. dir san.*, 2018, 1, 95, parag. 5, «mentre il trattamento dei dati genetici è inevitabile nelle ricerche di genetica molecolare, ossia all'interno di quelle ricerche dove si studia il DNA contenuto nelle cellule normali del corpo umano (come quelle circolanti nel sangue), esso è tendenzialmente da escludere nelle ricerche di patologia molecolare, ossia all'interno di quelle ricerche dove si studiano le cellule malate o alterate rispetto a quelle normali, in quanto in molti casi, come per esempio nelle cellule dei tumori, esse sono poco adatte a dare informazioni di tipo genetico, di modo che in una gran parte delle ricerche strettamente mediche effettuate ricorrendo allo strumento delle biobanche si analizzano solo dati sensibili (e non anche genetici)».

scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato» [13]. Tale disposizione potrebbe sembrare utile a regolare i casi di prelievo del campione solo per il suo impiego in una ricerca già approvata e non anche per la sua conservazione in vista di future sperimentazioni, perché l'archiviazione è riferita al pubblico interesse e la lett. g) distingue il pubblico interesse dal pubblico interesse di sanità pubblica, menzionato dalla lett. i). Ciò può portare a credere che l'archiviazione ex art. 9 non riguardi interessi sanitari. Invece, il considerando n. 53 del Regolamento europeo chiarisce che «[l]e categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, compreso il trattamento di tali dati da parte della dirigenza e delle autorità sanitarie nazionali centrali (…) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica». Dunque, il concetto di archiviazione nel pubblico interesse ex art. 9 include la raccolta anche ai fini di interesse sanitario. E si tratta di raccolta compatibile con quella posta in essere dalle biobanche. Infatti, l'ampia nozione di «archivio», accolta dall'art. 4, n. 6, include «qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico». In tale ambito, il legislatore nazionale ha introdotto ulteriori casi di trattamento senza consenso agli artt. 110 e 110-bis del codice della privacy.

Ove non si ritenesse rilevante la citata lett. j) dell'art. 9, il trattamento potrebbe comunque avvenire senza consenso, nel rispetto delle condizioni previste dalle lett. g) ed i), in quanto «necessario per motivi di interesse pubblico nel settore della sanità pubblica» [14], specie alla luce dell'ampia nozione di sanità pubblica indicata dal considerando n. 54 alla luce del Regolamento (CE) n. 1338/2008, o comunque perché «necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati

[13] M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ., comm.*, 2017, I, 165, parag. 4, rileva che il considerando n. 159 del Regolamento chiarisce l'ampia portata del concetto di finalità scientifica. Sul giudizio di proporzionalità si rinvia a S. Guida, D. Tozzi, *La valutazione della proporzionalità delle misure che limitano i diritti fondamentali della privacy nelle nuove linee guida del garante europeo della protezione dei dati*, in *Eur. j. privacy law tech.*, in http://www.ejplt.tatodpr.eu/Article/Archive/index_html?ida=185&idn=6&idi=-1&idu=-1.

[14] Proprio con questa giustificazione, motivata dalla «necessità di disporre con urgenza di studi epidemiologici e statistiche affidabili e complete sullo stato immunitario della popolazione, indispensabili per garantire la protezione dall'emergenza sanitaria in atto», il decreto legge 10 maggio 2020 n. 30, convertito, con modificazioni, dalla legge 2 luglio 2020, n. 72, recante «Misure urgenti in materia di studi epidemiologici e statistiche sul SARS-COV-2 (COVID-19)», ha «autorizzato il trattamento dei dati personali, anche genetici e relativi alla salute, per fini statistici e di studi scientifici svolti nell'interesse pubblico nel settore della sanità pubblica, nell'ambito di un'indagine di sieroprevalenza condotta congiuntamente dai competenti uffici del Ministero della salute e dall'Istituto nazionale di statistica (ISTAT), in qualità di titolari del trattamento e ognuno per i profili di propria competenza».

membri». Infatti, l'art. 2-sexies, lett. u) del Codice della privacy, come modificato dal D.Lgs. n. 101/18 considera rilevante l'interesse pubblico connesso ai compiti del servizio sanitario nazionale.

L'art. 89, paragrafo 1, richiamato dalla citata lett. j) dell'art. 9, dispone che «[i]l trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo» [15]. Dunque, il trattamento senza consenso avviene lecitamente solo se il dato genetico o di salute viene ricavato da campione anonimo *ab origine* o successivamente anonimizzato, oppure, in subordine, pseudonimizzato. Inoltre, devono essere trattati solo i dati necessari per la ricerca, sussistendo altrimenti violazione del principio di minimizzazione. Tuttavia, in base all'allegato X inserito nel D.Lgs. 16/2010 dal D.Lgs. n. 256/2016, di «Attuazione della direttiva 2015/565/UE che modifica la direttiva 2006/86/CE per quanto riguarda determinate prescrizioni tecniche relative alla codifica di tessuti e cellule umani», l'anonimizzazione può avvenire solo da parte delle «organizzazioni responsabili dell'applicazione sull'uomo», ma non da parte della biobanca che raccoglie il campione [16]. Infatti, l'anonimizzazione dei campioni può vanificare parzialmente l'utilità della ricerca, specie negli studi longitudinali ed epidemiologici [17].

[15] C. Ricci, P. Ricci, *Le biobanche di ricerca: questioni e disciplina*, cit., nota 51, fanno notare che «esiste una vasta gamma di possibilità di identificazione di un soggetto da cui sono prelevati i campioni biologici, rappresentate dalla diretta identificabilità, dalla codificazione (o indiretta identificabilità), dalla criptazione, dall'anonimizzazione e dall'anonimia. Nel caso del campione biologico direttamente identificabile, il ricercatore sa – o può facilmente scoprire – l'identità del donatore, in quanto è direttamente legata o collegata ai campioni o dati, mentre per quello indirettamente identificabile o codificato, l'identità del donatore rimane sconosciuta al ricercatore ma può essere rintracciata dal fornitore del tessuto (il medico che tratta il soggetto, per esempio) attraverso un codice che identifica il tessuto. Quindi la corrispondenza tra codice e identità è fisicamente separata dai campioni e dati; e solo un numero esiguo di persone può collegare il codice all'identità. Con la criptazione, invece, il codice è trasformato in parecchi caratteri collegati al codice con l'intervento di terzi, che sarà richiesto per rintracciare l'identità dell'individuo. Nel caso di tessuto anonimizzato, il collegamento tra campioni/dati e l'identità dell'individuo è stato eliminato in modo irreversibile, mentre si parla di tessuti anonimi quando non c'è mai stata la possibilità di collegare campione e relativi dati ad una persona determinata». In merito, si rinvia a Comitato nazionale per la biosicurezza e le biotecnologie, *Linee guida per la certificazione delle biobanche*, 19 aprile 2006, cit., all. 3, p. 32.

[16] Il punto 4.11.1 del medesimo provvedimento, in merito alle informazioni da fornire agli interessati per il «Trattamento di dati genetici per finalità di ricerca scientifica e statistica», aggiunge di comunicare all'interessato «a) gli accorgimenti adottati per consentire l'identificazione degli interessati soltanto per il tempo necessario agli scopi della raccolta o del successivo trattamento (art. 25 Regolamento UE 2016/679); b) le modalità con cui gli interessati, che ne facciano richiesta, possono accedere alle informazioni contenute nel progetto di ricerca».

[17] Il punto 4.11.1 del medesimo provvedimento, in merito alle informazioni da fornire agli interessati per il «Trattamento di dati genetici per finalità di ricerca scientifica e statistica», aggiunge di comunicare all'interessato «a) gli accorgimenti adottati per consentire l'identificazione degli interessati soltanto per il tempo necessario agli scopi della raccolta o del successivo trattamento (art. 25 Regolamento UE 2016/679); b) le modalità con cui gli interessati, che ne facciano richiesta, possono accedere alle informazioni contenute nel progetto di ricerca».

Il fatto che la direttiva richieda l'identificazione del donatore mentre il Regolamento europeo imponga l'anonimizzazione o la pseudonimizzazione non può portare all'abrogazione della direttiva *in parte qua* per effetto del criterio cronologico. Infatti, «il principio *lex posterior generalis non derogat priori speciali* – che ha la sua ragione nella migliore e più adeguata aderenza della norma speciale alle caratteristiche della fattispecie oggetto della sua previsione) – non può valere, e deve quindi cedere alla regola dell'applicazione della legge successiva allorquando dalla lettera e dal contenuto di detta legge si evinca la volontà del legislatore di abrogare la legge speciale anteriore o allorquando la discordanza tra le due disposizioni sia tale da rendere inconcepibile la coesistenza fra la normativa speciale anteriore e quella generale successiva» [18]. Nel caso in esame, la volontà di abrogare la direttiva non appare sostenibile, perché imporre l'anonimato anche in fase di raccolta dei campioni potrebbe, come detto, essere pregiudizievole per l'attività di ricerca. Peraltro, tale differenza contenutistica non impedisce la coesistenza delle due disposizioni, che può essere raggiunta limitando l'identificazione al momento della raccolta del materiale biologico dal concedente ed applicando l'anonimizzazione o la pseudonimizzazione all'attività di ricerca.

Il fatto che il trattamento possa avvenire senza consenso non significa che anche l'informazione possa essere omessa. Infatti, in primo luogo, gli artt. 13 e 14, paragrafo 1, lett. c) del Regolamento europeo richiedono di informare sulla «base giuridica del trattamento», che può non essere il consenso. Inoltre, il paragrafo 2, lett. c) di tali disposizioni obbligano ad informare dell'esistenza del diritto di revocare il consenso solo «qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a)», ossia sul consenso, così confermando che le altre informazioni devono essere trasmesse all'interessato anche per i trattamenti che non presuppongono il consenso dell'interessato [19].

Tra le informazioni dovute figurano quelle sulle «finalità del trattamento» (artt. 13 e 14, paragrafo 1, lett. c) del Regolamento europeo). Dunque, il legislatore non fa riferimento ad «una o più specifiche finalità», come invece negli artt. 6 e 9, paragrafo 1, relativamente al trattamento basato sul consenso. Inoltre, la lett. c) degli artt. 13 e 14 è la medesima lettera che obbliga a comunicare la «base giuridica del trattamento». Tali riferimenti normativi inducono a sostenere che, quando il trattamento può prescindere dal consenso, le finalità non debbano necessariamente essere specifiche, ma possano essere genericamente riferite ad attività di ricerca genetica oppure biomedica, dato che gli studi del primo tipo comportano rischi peculiari rispetto agli altri del settore biomedico. Tale conclusione appare compatibile con il citato provvedimento del Garante della privacy del 5 giugno 2019, che, al punto 4.3, intitolato «informazioni agli interessati», richiama gli artt. 13 e 14 del Regolamento europeo e si limita a prevedere come ulteriori informazioni: «a) i risultati conseguibili anche in relazione alle notizie inattese che possono essere

[18] Cons. Stato, Ad. plen., 27 luglio 2016, n. 17, punto 11, ed ivi giurisprudenza ordinaria di legittimità richiamata.

[19] I.A. Caggiano, *Il consenso al trattamento dei dati personali tra nuovo Regolamento Europeo e analisi comportamentale*, cit., 20 s. e nota 42, rileva che «La trasparenza, oltre ad essere principio generale del trattamento (art. 5, par. 1, lett. *a*) è qualificazione dell'informazione che il titolare deve fornire all'interessato in ogni caso, anche ove il consenso non sia richiesto».

conosciute per effetto del trattamento dei dati genetici; b) la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale utilizzo di tali dati per ulteriori scopi» [20]. Dunque, neppure il Garante richiede informazioni su *specifici* scopi di ricerca.

1. La tutela del diritto all'identità e all'autodeterminazione.

La privacy non è l'unico valore da tutelare in questi casi. Lo riconosce anche il relativo Regolamento europeo, che, alle lettere g), i) e j) dell'art. 9, richiede l'adozione di misure appropriate per tutelare tutti i diritti fondamentali dell'interessato, non soltanto la sua riservatezza. Infatti, il materiale biologico contiene il genoma di una persona, cioè la sua identità, che fa parte dei diritti inviolabili tutelati dall'art. 2 Cost. [21].

Inoltre, l'art. 32, comma 2, Cost. riconosce la libertà di autodeterminazione in ordine ai trattamenti sanitari, che peraltro rientra nel diritto al rispetto della vita privata garantito ex art. 8 CEDU come interpretato dalla Corte europea. Da ultimo, anche la Carta dei diritti fondamentali dell'Unione europea ha riconosciuto all'art. 3 il diritto all'informazione e al libero consenso nell'ambito della medicina e della biologia, significativamente includendolo nel Titolo I, dedicato alla «dignità».

Dall'unione di tali principi sembra emergere il diritto del paziente di scegliere cosa consentire sia fatto dai medici *sul* proprio corpo, ma anche *con* il proprio corpo, ossia con le cellule, tessuti od organi che ne vengono prelevati [22].

Dunque, la privacy non è l'unico diritto che si contrappone all'interesse pubblico alla ricerca biomedica.

Tale affermazione trova conforto normativo anche a livello internazionale ed europeo. Infatti, l'art. 1 sia della Convenzione d'Oviedo sui diritti umani nella biomedicina [23] che del suo protocollo addizionale relativo alla ricerca biomedica indicano come propri obiettivi la protezione della dignità e dell'identità di tutti gli esseri umani nonché la garanzia, senza discriminazione, del rispetto della loro integrità e degli altri diritti e libertà fondamentali. Il medesimo approccio è stato ribadito dall'art. 1 della citata raccomandazione del Consiglio d'Europa. Infatti, il punto 135 del Rapporto esplicativo della

[20] Il punto 4.11.1 del medesimo provvedimento, in merito alle informazioni da fornire agli interessati per il «Trattamento di dati genetici per finalità di ricerca scientifica e statistica», aggiunge di comunicare all'interessato «a) gli accorgimenti adottati per consentire l'identificazione degli interessati soltanto per il tempo necessario agli scopi della raccolta o del successivo trattamento (art. 25 Regolamento UE 2016/679); b) le modalità con cui gli interessati, che ne facciano richiesta, possono accedere alle informazioni contenute nel progetto di ricerca».

[21] G. Ferrando, *Diritto e scienze della vita. Cellule e tessuti nelle recenti direttive europee*, in *Familia*, 2005, 5, 1157, parag. 6.

[22] Ciò non toglie che il legislatore possa imporre l'uso dei campioni per determinate ricerche, così come obbligare ai trattamenti sanitari necessari nell'interesse sia del singolo che della collettività. Infatti, relativamente alla citata ricerca resa necessaria dall'emergenza sanitaria da Covid-19, l'art. 1, comma 6, D.L. 10 maggio 2020 n. 30, convertito nella legge n. 72/2020, dispone che «Il trattamento dei campioni e dei relativi dati è effettuato per esclusive finalità di ricerca scientifica sul SARS-COV-2 individuate dal protocollo di cui al comma 1, nel rispetto delle prescrizioni del Garante per la protezione dei dati personali individuate nel provvedimento del 5 giugno 2019».

[23] Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo 4 aprile 1997, in http://conventions.coe.int/Treaty/ita/Treaties/Html/164.htm.

Convezione, relativamente all'art. 22 sull'uso della parte staccata del corpo umano, chiarisce che «[e]ven when the sample is anonymous the analysis may yield information about identity» [24]. Dunque, l'interesse pubblico alla ricerca biomedica deve essere bilanciato non solo con la riservatezza, ma anche con la dignità, l'identità, l'integrità fisica e la libertà di autodeterminazione delle persone a qualsiasi titolo coinvolte nella ricerca biomedica. La necessità del bilanciamento trova espressa conferma nell'art. 4 del Protocollo addizionale, rubricato «General rule», ai sensi del quale «Research shall be carried out freely, subject to the provisions of this Protocol and the other legal provisions ensuring the protection of the human being». Formulazione ripresa anche dal preambolo alla citata Raccomandazione del Consiglio d'Europa.

Il criterio con cui operare tale bilanciamento è indicato dall'art. 3 del Protocollo addizionale, in linea con l'art. 2 della Convenzione di Oviedo: «The interests and welfare of the human being participating in research shall prevail over the sole interest of society or science». Il Consiglio d'Europa ha fatto proprie anche queste parole nel preambolo della citata raccomandazione del 2016. Tale conclusione non appare in contrasto con il bilanciamento indicato dall'art. 89, parag. 2, del Regolamento privacy [25], perché tale disposizione consente di derogare solo ai diritti di opposizione, di rettifica, di limitazione del trattamento e di accesso a numerose informazioni, ma non anche ai diritti d'informazione ex artt. 13 e 14, e fa espressamente salve le garanzie di cui al paragrafo 1 [26].

2. Raccolta e utilizzo del materiale biologico.

La Convezione di Oviedo contiene importanti previsioni per applicare tale criterio generale alla raccolta e all'uso di cellule e tessuti a fini di ricerca. In virtù del suo art. 22, una parte del corpo può essere conservata ed utilizzata per un fine diverso rispetto a quello per il quale era stata espiantata solo conformemente al consenso informato. Quest'ultimo, in base all'art. 5 della Convenzione, deve essere libero, revocabile in qualsiasi momento e riferito ad uno specifico trattamento, di cui occorre comunicare il rapporto rischi-benefici.

[24] Explanatory Report Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, in http://conventions.coe.int/Treaty/EN/Reports/Html/164.htm. Nella medesima prospettiva sembra porsi la citata Raccomandazione, chiarendo che «Non-identifiable biological materials may be used in a research project provided that such use does not violate any restrictions defined by the person concerned before the materials have been rendered non-identifiable and subject to authorisation provided for by law» (art. 21, comma 4, rubricato «General rule» in apertura del capitolo «Use of biological materials in a research project»).

[25] L'art. 89, paragrafo 2, del Regolamento europeo sulla privacy recita: «Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità». La disomogeneità di normative che tale previsione rischia di creare è criticata, tra gli altri, da G. Chassang, T. Southerington, O. Tzortzatou, M. Boeckhout, S. Slokenberga, *Data portability in health research and biobanking*,in *Eur. data prot. Law rev.*, 2018, 3, 300.

[26] Ciò nonostante, il fatto che una fonte sovraordinata come l'art. 89, parag. 2, ammetta la deroga a diritti soggettivi rende impercorribile qualsiasi soluzione ermeneutica che comporti un sacrificio per l'interesse pubblico alla ricerca non strettamente necessario alla tutela dei diritti all'identità e all'autodeterminazione.

Questa regola generale del consenso ai trattamenti sanitari deve trovare un'applicazione più elastica nella materia in esame. Infatti, come chiarisce il citato rapporto esplicativo al punto 137, il consenso esplicito e specifico è necessario solo in alcuni casi, «in particular where sensitive information is collected about identifiable individuals» [27]. Dunque, *a contrario*, se il donatore non è identificabile, il consenso esplicito e specifico non è necessario. Ciò non vuol dire, tuttavia, che tale uso a fine di ricerca sia lecito, perché la privacy non è l'unico valore in gioco. Infatti, per evitare che il decorso del tempo renda impossibile rimettersi in contatto con il donatore e impedisca l'uso del campione, il consenso attuale può essere surrogato dalla mancata opposizione, ma l'informazione sul possibile futuro utilizzo del materiale per fini di ricerca diversi da quelli per cui è stato acquisito deve comunque essere fornita [28].

La Convenzione di Oviedo non è formalmente diventata vincolante in Italia perché, sebbene ratificata con la legge n. 145/2001, tale strumento non è stato depositato. Ciononostante, la Suprema Corte ha chiarito che i principi contenuti in tale Convenzione devono essere intesi come criteri interpretativi per risolvere le questioni controverse, specie in mancanza di una disciplina *ad hoc* [29].

È, invece, vincolante, sebbene solo nei fini, la citata direttiva 2004/23/EC, che, pur riguardando espressamente cellule e tessuti umani, non disciplina dettagliatamente il contrasto tra libertà di ricerca e tutela dei diritti umani. L'art. 13 si limita a prevedere che: «1. L'approvvigionamento di tessuti o cellule umani è autorizzato solo se sono soddisfatti tutti i requisiti obbligatori relativi al consenso o all'autorizzazione in vigore nello Stato membro interessato. 2. Gli Stati membri, in conformità alla normativa nazionale, adottano tutte le misure necessarie per assicurare che i donatori, i loro congiunti o le persone che danno l'autorizzazione per conto dei donatori ricevano tutte le informazioni appropriate di cui all'allegato». L'Italia ha attuato tale direttiva con il D.lgs. n. 191/2007, senza apportare sostanziali integrazioni [30].

---

[27] Il consenso deve essere preceduto da un'appropriata consulenza genetica prima di procedere a test predittivi di malattie genetiche o che consentano di identificare la presenza di geni predisponenti a malattie (art. 12 della Convenzione e punto 88 del Rapporto esplicativo).

[28] Come si legge al punto 137 del Rapporto esplicativo, «sometimes, it will not be possible, or very difficult, to find the persons concerned again in order to ask for their consent. In some cases, it will be sufficient for a patient or his or her representative, *who have been duly informed* (for instance, by means of leaflets handed to the persons concerned at the hospital), not to express their opposition» (corsivo aggiunto). Nella stessa prospettiva, ma ancor più chiaramente, si pone la Raccomandazione del 2016, secondo cui «Prior to consent to or authorisation for the storage of biological materials for future research, the person concerned should be provided with comprehensible information that is as precise as possible with regard to: – the nature of any envisaged research use and the possible choices that he or she could exercise; – the conditions applicable to the storage of the materials, including access and possible transfer policies; and – any relevant conditions governing the use of the materials, including re-contact and feedback» (art. 10, rubricato «Information», ad apertura del capitolo III, intitolato «Obtaining and storage for future research»).

[29] Cass. civ., Sez. I, 16 ottobre 2007, n. 21748, relativa al noto caso Englaro, di interruzione della nutrizione artificiale, in http://www.altalex.com/index.php?idnot=38683. L'elenco dei Paesi in cui la Convenzione è entrata in vigore è consultabile all'indirizzo https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/164/signatures?p_auth=zNzPe3SG.

[30] L'art. 13 D.Lgs. n. 191/2007 dispone, infatti, che: «1. L'approvvigionamento di tessuti o cellule umani è consentito solo se sono soddisfatti tutti i requisiti previsti dalla normativa vigente in ordine al consenso informato o all'espressione di volontà o all'autorizzazione alla donazione. 2. Con decreto del Ministro della salute, d'intesa con la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, sono fissate le misure necessarie per garantire che i donatori, i

Ai sensi dell'allegato alla direttiva 2004/23, le informazioni devono precedere l'approvvigionamento e «comprendere: scopo e natura dell'approvvigionamento, sue conseguenze e rischi; esami analitici, se effettuati; registrazione e protezione dei dati del donatore, riservatezza medica; scopo terapeutico e potenziali benefici, nonché informazioni sulle salvaguardie applicabili volte a tutelare il donatore». Inoltre, il compito di comunicare le informazioni deve essere affidato a «persona qualificata, capace di trasmetterle in modo chiaro e adeguato, usando termini facilmente comprensibili per il donatore» [31].

L'allegato IV al D.Lgs. n. 16/2010 ha integrato il processo informativo

---

loro congiunti o le persone che danno l'autorizzazione per conto dei donatori, ricevano, oltre a tutte le informazioni previste dalle norme vigenti, anche quelle di cui all'allegato al presente decreto».

[31] Annex to Directive 2004/23/EC, Information To Be Provided on the Donation of Cells and/or Tissues, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:102:0048:0058:en:PDF.

Ben maggiori sono le informazioni che sarebbero necessarie per tutelare la libertà di autodeterminazione del concedente. Come rilevano, C. Ricci, P. Ricci, *Le biobanche di ricerca: questioni e disciplina*, cit., parag. 4, «il modulo con cui si propone ad una persona di accettare il prelievo di un campione e la sua successiva conservazione ed utilizzazione a fini di ricerca dovrebbe indicare nella maniera più precisa possibile: 1) gli scopi del prelievo; 2) gli scopi della conservazione; 3) le modalità con cui il prelievo avverrà e le loro eventuali implicazioni più significative per l'organismo; 4) i riferimenti sul luogo geografico deputato alla conservazione; 5) le modalità con cui verrà garantita la sicurezza circa la conservazione dei dati e la *privacy*; 6) le modalità con cui gli interessati che ne facciano richiesta possono accedere alle informazioni contenute nel progetto di ricerca; 7) la durata dello stoccaggio; 8) le modalità con cui potrà essere eventualmente modificato o revocato il consenso ed, in tal caso, presentata l'eventuale richiesta di distruzione del campione; 9) le indennità previste nel caso di danno causato dalla partecipazione allo studio; 10) la destinazione del campione nel caso di decesso del soggetto; 11) i risultati conseguibili, anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici, e la loro comunicabilità o meno al diretto interessato; 12) l'eventualità che i dati e/o i campioni biologici siano conservati e utilizzati per altri scopi di ricerca scientifica e statistica, per quanto noto, adeguatamente specificati, anche con riguardo alle categorie di soggetti ai quali possono essere eventualmente comunicati i dati oppure trasferiti i campioni; 13) nel caso in cui sia previsto il trasferimento di dati genetici e di campioni anche in Paesi non appartenenti all'Unione europea, la presenza in tali Paesi di un livello di tutela delle persone adeguato, nonché gli estremi identificativi dei soggetti destinatari dei dati e dei campioni, al fine di garantire in concreto all'interessato la possibilità di esercitare il controllo sui dati e sui campioni che lo riguardano; 14) l'assenza di qualsiasi diritto di partecipazione, su base individuale, agli eventuali profitti derivanti dallo studio dei campioni biologici; 15) l'effettivo ruolo svolto dallo sponsor o promotore della ricerca (o dai suoi collaboratori) e l'assenza di un conflitto di interesse tra questi e gli sperimentatori; 16) l'identità e i dati di contatto del titolare del trattamento; 17) il diritto dell'interessato di chiedere al titolare del trattamento la rettifica dei dati o la limitazione del trattamento; 18) il diritto di proporre reclamo innanzi alle competenti autorità di controllo in caso di illecito trattamento dei dati.

Anche nelle ipotesi in cui i materiali biologici siano stati già rimossi per scopi estranei alla ricerca, tra l'altro molto frequenti dal momento che i tessuti molto spesso vengono asportati nell'ambito di operazioni chirurgiche e diagnostiche condotte per altri fini, il consenso dovrà essere ottenuto preferibilmente prima del prelievo dei campioni biologici e, benché effettuato per altre e diverse finalità rispetto a quelle di ricerca, riguarderà nello specifico anche l'immagazzinamento e l'uso dei campioni biologici per tali scopi» (note omesse).

Più sintetico è l'elenco di informazioni indicato nel parere congiunto del Comitato nazionale di bioetica e del Comitato nazionale per la biosicurezza, le biotecnologie e le scienze della vita, *Raccolta di campioni biologici a fini di ricerca: consenso informato* (Presidenza del Consiglio dei Ministri, Roma, 16 febbraio 2009, in http://bioetica.governo.it/media/3457/p2009-misto-2-raccolta-di-campioni-biologici-a-fini-di-ricerca-consenso-informato-it.pdf, pag. 9), i quali, tuttavia, menzionano opportunamente la partecipazione volontaria, l'eventuale trasferimento dei campioni ad altra banca, o a gruppi di ricerca diversi dal proponente, la possibilità o l'esclusione di un ritorno d'informazione al donatore sui risultati della ricerca, (esclusione che si può realizzare quando l'indagine sul materiale genetico non ha un significato "clinico"), le indicazioni sulle possibili conseguenze per il donatore od i membri della sua famiglia dei risultati delle analisi genetiche, e la possibilità di rendere anonimi i campioni o di identificarli con un codice. Sulle tecniche per evitare che la complessità dell'informativa pregiudichi l'effettiva consapevolezza della scelta dell'interessato, si rinvia a L. Aulino, *Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come un rimedio ex ante*, in *Dir. informazione e informatica*, 2020, 2, 303-312.

precisando che «il medico responsabile della selezione, o personale sanitario appositamente formato operante sotto la responsabilità del predetto, che raccoglie informazioni sull'anamnesi, si accerta che il donatore nel corso del colloquio: a) abbia compreso le informazioni fornite; b) abbia avuto l'opportunità di porre domande e abbia ricevuto risposte esaurienti; c) abbia confermato che tutte le informazioni e le risposte fornite sono veritiere».

Nonostante quest'integrazione, le direttive europee e i loro decreti d'attuazione italiani restano lacunosi riguardo ai tipi di consenso informato che è obbligatorio acquisire. Quattro sono i modelli di riferimento: a) specifico, perché valevole per una determinata ricerca o trattamento; b) parzialmente ristretto, ossia relativo ad una ricerca determinata, ma anche ai suoi sviluppi e alle indagini potenzialmente associate in futuro direttamente o indirettamente; c) multi-opzione, che include più trattamenti e ricerche individuati; d) ampio, perché prestato senza indicazione specifica dei trattamenti e delle ricerche [32].

Le direttive europee non sembrano collegare il consenso ad una determinata ricerca, neppure nel senso elastico del modello parzialmente ristretto. Infatti, l'allegato IV della citata direttiva 2006/17, al punto 2.4, riporta, tra i dati che l'istituto dei tessuti deve registrare, «l'assenso o autorizzazione, in particolare lo scopo per cui possono essere impiegati i tessuti e le cellule (ovvero uso terapeutico o uso di ricerca, oppure uso sia terapeutico che di ricerca) e qualsiasi istruzione specifica relativa all'eliminazione se i tessuti o le cellule non sono utilizzati per lo scopo a cui erano destinati». Dunque, il consenso non sembra riferito ad un uso determinato, bensì agli usi rientranti negli scopi terapeutici o di ricerca.

Altrettanto non percorribile appare la soluzione del consenso ampio, già sul piano dell'ordinamento europeo. L'obbligo di informazione previsto dalla direttiva 2004/23, infatti, non include solo lo «scopo», ma anche la «natura dell'approvvigionamento, sue conseguenze e rischi». Questi ultimi, come detto, sono maggiori in caso di ricerca genetica. Quindi, l'informazione deve tenerne conto e non può essere uguale a quella relativa a ricerche biomediche che non riguardano geni e cromosomi. Di conseguenza, il consenso non può essere talmente ampio da consentire l'uso del campione indifferentemente per gli studi genetici o per le altre ricerche biomediche. Inoltre, il riferimento alle conseguenze, specie perché distinto da quello allo scopo e ai rischi, sembra poter includere gli utilizzi cui il campione potrebbe essere destinato nel tempo nell'ambito della generica finalità di ricerca.

Alla medesima conclusione si può giungere a livello di ordinamento interno. Un primo argomento contro la validità del consenso ampio potrebbe derivare dalla sua natura. Al riguardo, il fatto che il consenso presupponga, oltre alla capacità naturale, l'informazione sulle conseguenze del trattamento sembra implicare una volontà non solo dell'atto, ma anche dell'effetto. Il che porta ad attribuire al consenso natura negoziale. Di conseguenza, il consenso ampio, lasciando all'utilizzatore la scelta su come impiegare il campione, gli rimette la determinazione dell'oggetto del negozio, con conseguente rischio di ledere il

[32] D. Farace, *Campioni biologici*, cit., p. 2.

principio dell'accordo [33]. Tuttavia, anche a voler intendere il negozio come bilaterale in ragione dei contrapposti obblighi di custodia assunti dalla biobanca [34], tale lesione dovrebbe essere esclusa quando vi sono limiti alla discrezionalità della parte cui è rimessa la determinazione dell'oggetto o comunque la sua scelta risulta ragionevolmente prevedibile sulla base di parametri obiettivi [35]. Nel caso in esame, l'esistenza di limiti normativi che impediscono determinate ricerche e la possibilità per l'interessato, anche nel consenso ampio, di indicare finalità di ricerca alle quali si oppone appaiono strumenti idonei ad evitare che il consenso ampio diventi fonte di abusi dell'utilizzatore.

Altri riferimenti normativi sembrano meno controvertibili. Il provvedimento del 2019 del Garante della privacy conferma numerose limitazioni alla possibilità di destinare il campione a finalità di ricerca diverse da quelle per le quali è stato acquisito [36]. Il che è incompatibile con il modello del consenso ampio.

In secondo luogo, il consenso all'uso del campione biologico è un atto di disposizione del proprio corpo [37]. Quindi, è invalido ex art. 5 c.c. se contrario alla legge, come, ad esempio, il consenso ad utilizzare una propria cellula somatica attraverso il trasferimento del suo nucleo «in una cellula uovo animale privata del nucleo, ma nella quale restano presenti i mitocondri animali» [38], così da ottenere ibridi citoplasmatici (c.d. cibridi) in violazione del divieto di

[33] Sull'applicabilità della disciplina negoziale agli atti di disposizione del corpo si rinvia a A. Galasso, *Biotecnologie e atti di disposizione del corpo*, in *Familia* 2001, 4, 925-936; C.M. D'Arrigo, *Il contratto e il corpo: meritevolezza e liceità degli atti di disposizione dell'integrità fisica*, in *Familia*, 2005, 4-5, 777; G. Resta, *Autonomia privata e diritti della personalità*, Jovene, Napoli, 2005.

[34] A sostegno della natura di negozio autorizzatorio unilaterale, si rinvia alle considerazioni di G. Resta, *La disposizione del corpo. Regole di appartenenza e di circolazione*, in S. Rodotà, P. Zatti (diretto da), *Trattato di biodiritto*, Vol. II, t. I, *Il governo del corpo*. Giuffrè, Milano, 2011 809-848.

[35] V. Roppo, *Il contratto*, Giuffrè, Milano, 2011, 338.

[36] Garante della privacy, Provvedimento del 5 giugno 2019, cit., punto 4.11.3, seconda parte, secondo cui «Quando a causa di particolari ragioni non è possibile informare gli interessati malgrado sia stato compiuto ogni ragionevole sforzo per raggiungerli, la conservazione e l'ulteriore utilizzo di campioni biologici e di dati genetici raccolti per la realizzazione di progetti di ricerca e indagini statistiche, diversi da quelli originari, sono consentiti se una ricerca di analoga finalità non può essere realizzata mediante il trattamento di dati riferiti a persone dalle quali può essere o è stato acquisito il consenso informato e: aa) il programma di ricerca comporta l'utilizzo di campioni biologici e di dati genetici che in origine non consentono di identificare gli interessati, ovvero che, a seguito di trattamento, non consentono di identificare i medesimi interessati e non risulta che questi ultimi abbiano in precedenza fornito indicazioni contrarie; bb) ovvero il programma di ricerca, preventivamente oggetto di motivato parere favorevole del competente comitato etico a livello territoriale, è sottoposto a preventiva consultazione del Garante ai sensi dell'art. 36 del Regolamento (UE) 2016/679».

[37] In senso contrario, M. Macilotti, *Proprietà, informazione ed interessi nella disciplina delle biobanche a fini di ricerca*, in *Nuova giur. civ. comm*.., 2008, II, 226, rileva che «una volta asportati dal corpo, i tessuti umani non conservino alcun legame materiale con il corpo di cui erano parte. Gli interventi e le ricerche effettuati sui tessuti dopo l'ablazione, non hanno alcuna influenza diretta sulla salute del soggetto che ha subito l'asportazione del campione. Il che esclude la rilevanza dell'art. 5 cod. civ. nell'ipotesi in esame, in quanto tale norma regola gli atti di disposizione del proprio corpo inteso nella sua unità, ma perde efficacia quanto il campione diviene altro dal corpo-soggetto». Questa tesi sarebbe condivisibile se l'effetto menomativo permanente sulla salute fosse l'unico limite all'atto di disposizione. Quest'ultimo, invece, è vietato anche se in contrasto con la legge, con l'ordine pubblico o con il buon costume. Ed è irrilevante che la violazione di legge avvenga disponendo di una parte del corpo che deve ancora essere asportata oppure di un campione già prelevato. Dunque, l'asportazione del materiale biologico non esclude l'applicazione dell'art. 5 c.c.

[38] Comitato nazionale per la bioetica, *Chimere ed ibridi con una riflessione particolare sugli ibridi citoplasmatici*, 26 giugno 2009, p. 3, in http://bioetica.governo.it/media/1857/p842009chimereedibridiit.pdf

produzione di ibridi ex art. 13, commi 4 e 3, lett. d), legge n. 40/2004 [39]. Dunque, occorre verificare la validità dell'atto di disposizione. Ma ciò è possibile solo se il consenso ha un contenuto determinato o determinabile [40]. Quindi, l'unico tipo di consenso compatibile sia con l'ordinamento nazionale che con quello europeo sembra essere quello multi-opzione.

Peraltro, proprio gli indicati e stringenti limiti all'uso dei campioni per scopi diversi da quelli originari comportano la necessità che il consenso iniziale non sia ristretto o parzialmente ristretto. Infatti, poiché la libertà della ricerca è tutelata sia dall'art. 9 Cost. che dall'art. 13 della Carta dei diritti dell'Unione europea, le limitate possibilità di utilizzo dovute a tali modelli dovrebbero essere controbilanciate dalla possibilità di chiedere nuovamente il consenso per ulteriori ricerche agli originari concedenti. Invece, tale possibilità è subordinata alle ristrette condizioni riportate al punto 4.11.3 dell'indicato provvedimento del Garante. Di conseguenza, il necessario bilanciamento tra diritti individuali ed interesse pubblico alla ricerca comporta che tale rigidità sia compensata da una maggior elasticità nell'utilizzo in base al consenso ottenuto al momento del prelievo. La conseguenza sembra essere la maggior compatibilità costituzionale del modello multi-opzione.

3. Circolazione del materiale biologico.

La circolazione del materiale biologico ne consente l'uso da parte di soggetti diversi rispetto a quelli che raccolgono il campione. Come per la raccolta, anche la circolazione può avere fonte legale (non regolamentare, vertendosi in materia di trattamenti sanitari obbligatori o comunque di «prestazione personale» ex art. 23 Cost. [41]) o negoziale. Un esempio della prima è rappresentato dall'art. 1, comma 7, D.L. 10 maggio 2020, n. 30, convertito nella legge n. 72/2020, il quale dispone che i dati raccolti nell'ambito della menzionata ricerca autorizzata dal medesimo decreto, privi di identificativi diretti, possono essere comunicati, per finalità scientifiche, agli enti ed agli uffici del Sistema statistico nazionale (Si.Sta.N) e agli ulteriori soggetti individuati con decreto di natura non regolamentare del Ministro della salute, d'intesa con il Presidente dell'ISTAT, sentito il Garante per la protezione dei dati personali, nel rispetto dell'articolo 5-ter del D.Lgs. n. 33 del 2013 e previa stipula di appositi protocolli di ricerca da parte dei soggetti incaricati di

[39] Sul processo di marginalizzazione subito dall'art. 5 c.c. si rinvia a G. Ferrando, *Il principio di gratuita, bioetcnologie e «atti di disposizione del proprio corpo»*, in *Europa dir. priv.*, 2002, 3, 765 ss., la quale ritiene fuorviante la categoria degli atti di disposizione e «più appropriata quella degli "atti di destinazione", in quanto è la destinazione ad uno scopo (la salute del ricevente) e, talvolta, anche ad un destinatario identificato, quel che immediatamente caratterizza il "dono" di una parte di sé». Poiché anche gli atti di destinazione non possono essere validi se in contrasto con la legge, il processo di marginalizzazione dell'art. 5 c.c. non sembra poter mettere in dubbio l'invalidità del consenso ampio.

[40] Come rileva D. Farace, *Campioni biologici*, cit., p. 2, «parrebbe sempre necessaria un'indicazione degli scopi o degli impieghi, per evitare di cadere nell'indeterminabilità e, di conseguenza, nell'invalidità per carenza di precisa e puntuale informazione».

[41] L'art. 224-bis c.p.p. considera «atti idonei ad incidere sulla libertà personale» il prelievo di capelli o di mucosa, ossia la raccolta del campione biologico. Di conseguenza, poiché la prestazione non consiste solo nel sottoporsi al prelievo, ma anche nel destinarlo a determinati utilizzatori, il legislatore sembra imporre una prestazione personale sia quando obbliga al prelievo sia quando prevede che il campione consensualmente espiantato sia destinato ad utilizzatori che il paziente non può scegliere.

svolgere tale indagine per effetto del comma 1.

In mancanza di una legge, la legittimazione dei terzi all'uso del campione biologico presuppone la sua cessione da parte della biobanca che lo conservava. Il *favor* europeo per la circolazione del materiale biologico emerge chiaramente dal considerando n. 53 del Regolamento privacy, secondo cui «Gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi».

Anche l'art. 18 della Raccomandazione del 2016 invita gli Stati a facilitare l'accesso dei ricercatori alle collezioni di materiali biologici, perché, come emerge dal suo preambolo, la ricerca è spesso interdisciplinare ed internazionale e, quindi, la condivisione dei campioni al di là dei confini nazionali diventa fondamentale.

Di conseguenza, in primo luogo, il criterio ermeneutico da applicare nella soluzione delle questioni controverse deve essere quello favorevole alla possibilità dei ricercatori di accedere al materiale biologico. Inoltre, le limitazioni alla possibilità di acquisire, utilizzare e trasferire il materiale biologico non dovrebbero essere applicate analogicamente.

Tuttavia, la circolazione del campione biologico è influenzata dalla natura del diritto trasferito dal concedente. Se si trattasse di un diritto di proprietà, la biobanca potrebbe disporre del campione a favore di terzi a prescindere dalla volontà del concedente. Se la posizione della banca fosse paragonabile a quella dell'usufruttuario, potrebbe trasferire il materiale previa notifica al soggetto da cui è stato prelevato, in applicazione dell'art. 980 c.c. Se, invece, si è al di fuori dell'area della realità, il trasferimento del campione biologico dalla biobanca all'utilizzatore non sembra configurare una cessione di credito, con conseguente applicazione dell'art. 1264 c.c. Infatti, il cessionario non subentra soltanto nel diritto di utilizzare il campione, ma anche negli obblighi di custodia e di riservatezza. Quindi, sembra verificarsi una cessione della complessiva posizione negoziale che ha la biobanca nei confronti del soggetto originario concedente, ossia del ceduto. Ne deriva la necessità di acquisire il consenso di quest'ultimo, in applicazione (analogica, perché siamo al di fuori dell'area del contratto in senso stretto) dell'art. 1406 c.c.

La tesi della natura reale del diritto della biobanca non appare condivisibile [42]. In primo luogo, il materiale biologico destinato ad attività di ricerca è materia vivente umana [43]. Di conseguenza, non può essere oggetto di un diritto di proprietà in capo a terzi, tanto più in un ordinamento che, come quello

[42] A sostegno della tesi secondo cui le parti staccate del corpo sono oggetto di un diritto di proprietà, si rinvia a O.T. Scozzafava, *I beni e le forme giuridiche dell'appartenenza*, Giuffrè, Milano, 1982, 602.

[43] P. D'Addino Serravalle, *Corpo (atti di disposizione del)*, in *Enc. bioetica e scienza giur.*, vol. III, Ed. Scientifiche Italiane, Napoli, 2010, 547; M.C. Venuti, *Atti di disposizione del proprio corpo*, Giuffrè, Milano, 2002, 219 s.; G. Resta, *Do we own our bodies? Problemi in tema di utilizzazione del materiale biologico umano a scopi di ricerca e brevettazione*, in AA.VV., *Studi in onore di Nicolò Lipari*, Giuffrè, Milano, vol. II, 2008, 2451. Peraltro, come rileva M. Tamponi, *Campioni biologici e atti di disposizione del corpo*, in D. Farace (a cura di), *Lo statuto etico-giuridico dei campioni biologici umani*, atti del convegno organizzato dall'Università di Tor Vergata, 7 luglio 2016, Nuova Editrice Universitaria, Roma, 2016, 213, «anche ad ammettere che il corpo privo di vita venga attratto dal mondo dell'essere a quello dell'avere, la sua reificazione non consentirebbe di ricondurlo in tutto e per tutto allo schema dominicale, fino a fare di esso un mero e qualsiasi bene *ex* art. 810 cod. civ.».

italiano, attribuisce alla proprietà una funzione sociale addirittura in Costituzione. Affermare la funzione sociale delle parti staccate del corpo appare incompatibile con il carattere personalistico della Costituzione.

Inoltre, il diritto di godimento del proprietario e dell'usufruttuario è pieno, quindi incompatibile con il diritto di utilizzo concesso alla biobanca, il quale, invece, è comunque limitato perché, come detto, il consenso ampio non è previsto né dall'ordinamento europeo né da quello interno.

Peraltro, il diritto reale non può sorgere in capo alla biobanca neanche attraverso l'uso del campione. Infatti, il Garante della privacy ha ribadito nel 2019 che «In caso di revoca del consenso da parte dell'interessato, i trattamenti devono cessare e i dati devono essere cancellati o resi anonimi anche attraverso la distruzione del campione biologico prelevato» [44]. Dunque, a prescindere dalla questione se il potere di revoca sia soggetto a limiti quantomeno di buona fede e di tutela dell'affidamento [45], si esclude che l'uso del campione nel tempo possa far sorgere diritti in capo all'ente di ricerca [46].

In quarto luogo, tale disposizione del provvedimento del Garante della privacy fa emergere che l'attribuzione alla biobanca di un diritto reale sul campione determinerebbe una violazione del principio di tipicità dei diritti reali. Infatti, un diritto reale soggetto ad estinzione per effetto della revoca del consenso traslativo non corrisponde ad alcuna delle figure tipiche previste dall'ordinamento.

Appare, quindi, preferibile sostenere che il trasferimento del campione a terzi possa avvenire solo nel rispetto della libertà di autodeterminazione della persona cui si riferisce quel campione [47]. Ne deriva che la circolazione del materiale biologico presuppone il consenso del soggetto da cui viene prelevato.

A sostegno di tale conclusione depongono alcuni dati normativi. L'art. 170-

---

[44] Garante della privacy, Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101, cit., punto 4.5.1.

[45] A sostegno della necessità di ulteriori limiti al potere di revoca, anche in considerazione della diversità tra ricerca su campioni biologici e sperimentazione sull'uomo, si rinvia a M. Macilotti, *Consenso informato e biobanche di ricerca*, in *Nuova giur. civ. comm.*, 2009, II, 164 s.

[46] Con il provvedimento del 2019, quindi, il Garante conferma il legame esistente tra campione e concedente, già affermato dalle autorizzazioni generali al trattamento dei dati genetici n. 8/2013 e n. 8/2016, secondo le quali «Nel caso in cui l'interessato revochi il consenso al trattamento dei dati per scopi di ricerca, è distrutto anche il campione biologico sempre che sia stato prelevato per tali scopi, salvo che, in origine o a seguito di trattamento, il campione non possa più essere riferito ad una persona identificata o identificabile». Tale distinzione tra persona identificabile e non identificabile risulta eliminata nel sopra riportato testo vigente, il che riduce ulteriormente i poteri dell'utilizzatore sul campione e corrobora la tesi secondo cui essi trovano fondamento e confini nel consenso del concedente.
In senso contrario, secondo R. Pacia, *Campione biologico e consenso informato nella ricerca genetica: il possibile ruolo delle biobanche*, in www.iuscivile.it, 2014, 3, 80, il legame tra campione e utilizzatore troverebbe conferma nell'impossibilità per il concedente di chiedere la restituzione del campione, in quanto rifiuto sanitario pericoloso ai sensi dell'art. 45, d.lgs. 15 febbraio 1997, n. 22 (*Disciplina sulla gestione dei rifiuti*) e del d.p.r. 15 luglio 2003, n. 254 (*Regolamento recante la disciplina della gestione dei rifiuti sanitari*). Tuttavia, il fatto che la revoca del consenso impedisca la prosecuzione dell'uso del campione denota una chiara prevalenza, nel rapporto con il materiale biologico, della posizione del concedente rispetto a quella dell'utilizzatore. E l'impossibilità di ottenerne la restituzione si spiega adeguatamente con la pericolosità del campione, senza alcuna necessità di desumerne anche l'insussistenza di diritti del concedente sul proprio materiale biologico.

[47] Come rileva G. Cricenti, *I diritti sul corpo*, Jovene, Napoli, 2008, 190, «Il consenso non vale a rendere lecito il prelievo a fini terapeutici o scientifici di materiale umano (ad esempio cellule), poiché quel prelievo è lecito di suo; ma vale a rendere lecito lo sfruttamento in proprio fatto dal ricercatore dei risultati di quel prelievo; vale a determinare gli ambiti del diritto di terzi sul corpo del soggetto e sulle sue parti».

bis, comma 3, D.Lgs. 10 febbraio 2005, n. 30 (G.U. n. 52 del 4 marzo 2005) dispone che «La domanda di brevetto relativa ad una invenzione che ha per oggetto o utilizza materiale biologico di origine umana deve essere corredata dell'espresso consenso, libero e informato, a tale prelievo e utilizzazione, della persona da cui è stato prelevato tale materiale, in base alla normativa vigente» [48]. Tale disposizione appare pertinente perché l'invenzione brevettabile presuppone l'attività di ricerca scientifica [49]. Quindi, è innanzitutto quest'ultima a necessitare del consenso libero e informato. Tanto più che si tratta di un requisito funzionale al rispetto dei diritti del paziente, non all'utilità dell'invenzione. A corroborare la rilevanza di tale obbligo concorre l'ingente sanzione amministrativa pecuniaria (da 100.000 a 1.000.000 di euro) prevista dall'art. 170-ter del medesimo decreto [50].

Dal comma 3 dell'art. 170-bis sembra emergere anche un altro dato. Un consenso manifestato senza informazione circa l'uso che si farà del campione non è valido. La persona che consente al prelievo non può rinunciare all'informazione circa l'uso cui è destinato il campione, a differenza di quanto prevede l'art. 1 legge n. 219/17 per i trattamenti diagnostico-terapeutici [51]. La *ratio* di questa *lex specialis* sembra risiedere, in primo luogo, nella necessità che l'interesse collettivo alla ricerca sia controbilanciato dalla più piena tutela dell'interesse individuale all'informazione, ma anche nel dovere di sapere a cosa si contribuisce con il proprio corpo, perché potrebbe trattarsi di finalità illegali, come nell'indicato esempio della produzione di cibridi. L'indisponibilità del diritto all'informazione corrobora la tesi che i diritti dell'utilizzatore trovino i propri limiti e fondamento nel consenso informato della persona da cui i campioni sono prelevati [52].

In tal senso sembra deporre anche il punto 4.3. del citato parere del Garante del 5 giugno 2019, secondo cui «Le informazioni da rendere agli interessati ai sensi degli artt. 13 e 14 Regolamento (UE) 2016/679 e anche ai sensi degli artt. 77 e 78 del Codice per il medico di medicina generale e per il pediatra di libera scelta, evidenziano, altresì: (…) b) la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale utilizzo di tali dati per ulteriori scopi». Dunque, da un lato, la circolazione sia dei dati che del materiale biologico presuppone il consenso; dall'altro, l'interessato può scegliere di non limitare

[48] Interessante la storia di questa disposizione, ricostruita da R. Pacia, *Campione biologico e consenso informato nella ricerca genetica: il possibile ruolo delle biobanche*, cit., 84, cui si rinvia.
[49] La rilevanza di tale disposizione è sostenuta anche da C. Ricci, P. Ricci, *Le biobanche di ricerca: questioni e disciplina*, cit., nota 43.
[50] Tale sanzione si applica a «chiunque, al fine di brevettare una invenzione, utilizza materiale biologico di origine umana, essendo a conoscenza del fatto che esso è stato prelevato ovvero utilizzato per tali fini senza il consenso espresso di chi ne può disporre».
[51] Il codice di deontologia medica aveva già da tempo identificato l'obbligo del medico di rispettare la documentata volontà del paziente di non essere informato. Sul punto, sia consentito il rinvio a G. Montanari Vergallo, *Il rapporto medico-paziente. Consenso e informazione tra libertà e responsabilità*, Giuffrè, Milano, 2008.
[52] Peraltro, anche quando l'utilizzatore è legittimato dalla legge, quest'ultima si pone comunque il problema dell'informazione della persona da cui proviene il campione. Infatti, l'art. 1, comma 6, ultima parte, D.L. n. 30/2020, convertito nella legge n. 72/2020, sancisce che «Gli interessati sono adeguatamente informati dei progetti di ricerca condotti sui campioni e sui dati presenti nella banca ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679». Analogamente, anche nell'ambito dei trattamenti sanitari obbligatori, l'art. 33, comma 4, legge n. 833/78 richiede che siano «accompagnati da iniziative rivolte ad assicurare il consenso e la partecipazione da parte di chi vi è obbligato».

tale circolazione.

Ai fini della consapevolezza di tale scelta non è tanto importante l'identità del terzo quanto sapere che si tratta di ente in possesso dei requisiti di accreditamento previsti dalle citate direttive europee ed obbligato ad usare il campione solo in ricerche previamente autorizzate da un comitato etico.

Conclusioni.

Raccolta, uso e circolazione di campioni biologici coinvolgono non soltanto la privacy del soggetto da cui vengono prelevati, ma anche l'identità, la dignità e la libertà di autodeterminazione in ordine alla propria integrità fisica, perché il distacco di una parte dal resto del corpo non può far venire meno il legame identitario che li unisce.

Da quest'approccio sembrano derivare due conseguenze.

In primo luogo, se, ai fini della disciplina in materia di privacy, l'anonimizzazione consente il trattamento del materiale biologico senza consenso, quest'ultimo e le relative informazioni restano necessari sia per la raccolta che per la conservazione e la circolazione, onde evitare la violazione dei menzionati diritti costituzionalmente tutelati. Infatti, anche se non è possibile risalire all'identità del donatore, si tratta comunque del materiale biologico di un essere umano. Quindi, anche dopo l'anonimizzazione, occorre sempre evitare di usare i campioni in modi o per finalità incompatibili con la volontà espressa a suo tempo dal loro donatore.

In secondo luogo, il campione non può essere reso anonimo senza un valido consenso informato. Diversamente, il donatore verrebbe privato sia del diritto di scegliere se destinare il proprio materiale biologico ad altre ricerche sia del diritto di revocare il consenso. Invece, l'autodeterminazione della persona, per essere piena e coerente con l'approccio personalista adottato dalla Costituzione italiana, deve estendersi anche all'uso delle parti staccate del proprio corpo in quanto ne condividono l'identità genetica [53].

D'altro canto, estendere pienamente alla raccolta, uso e circolazione del materiale biologico a fini di ricerca la logica del consenso specifico, propria dei trattamenti non sperimentali, sembra una soluzione eccessivamente generalizzante, incapace di tenere conto della peculiarità delle situazioni in esame. La ricerca scientifica rappresenta un valore di fondamentale importanza per il miglioramento delle condizioni di salute e, quindi, per la produttività di un Paese. Lo riconoscono, oltre all'art. 9 Cost. e all'art. 13 della Carta dei diritti fondamentali dell'Unione europea, sia il Protocollo addizionale alla Convenzione di Oviedo sia la Raccomandazione del 2016 nella parte in cui ribadiscono la libertà della ricerca. Inoltre, il suo avere ad oggetto campioni biologici comporta la mancanza di rischi per la salute del paziente da cui provengono, ad eccezione di quelli connessi all'intervento di prelievo, solitamente semplice o comunque già necessario per esigenze diagnostiche o terapeutiche. Di conseguenza, una semplificazione della procedura di acquisizione del consenso, come quella rappresentata dal consenso multi-

[53] G. Montanari Vergallo, A. di Luca, I. Catarinozzi, L. Iovenitti, N.M. di Luca, *Regulatory models of adult consent to the use of biological material in research biobanks*, in *Riv. it. med. leg. dir. san.*, 2016, 3, 1033-1049.

opzione, appare non solo più rispondente all'interpretazione letterale, teleologica e sistematica delle menzionate norme, ma anche più condivisibile nella doverosa ottica del bilanciamento tra interesse generale alla ricerca scientifica e tutela dei diritti individuali.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

La vulnerabilità tecnologica. Neurorights ed esigenze di tutela: profili etici e giuridici.

Technological vulnerability. Neurorights and protection requirements: ethical and legal profiles.

ANNA ANITA MOLLO
Assegnista di ricerca Università degli studi di Napoli Federico II

Abstract

Il contributo analizza il paradigma della vulnerabilità da un punto di vista etico e giuridico, nelle sue diverse declinazioni, rapportato alle fattispecie che sono il risultato dell'evoluzione tecnologica. Con specifico riferimento all'ambito delle neuroscienze, si analizzano le ricadute sulle categorie giuridiche tradizionali e sui diritti fondamentali derivanti dall'impiego di neurotecnologie. Si prospettano, infine, le possibili soluzioni da un punto di vista pratico, di integrazione tra la riflessione giuridica e la sperimentazione bio-ingegneristica.

The contribution analyzes the paradigm of vulnerability from an ethical and legal point of view in its various forms, related to the cases that are the result of technological evolution. With specific reference to the field of neuroscience, the contribution analyzes the repercussions on traditional legal categories and on fundamental rights deriving from the use of neurotechnologies. Finally, possible solutions are proposed from a practical point of view, of integration between legal reflection and bio-engineering testing.

Parole chiave: vulnerabilità; neuroscienze; neurotecnologie; neurodiritti; identità; privacy.

Keywords: vulnerability; neuroscience; neurotechnologies; neurorights; identiy; privacy.

Summary: Introduzione. L'inquadramento giuridico della "vulnerabilità": le difficoltà di classificazione e l'apporto della Corte Europea dei Diritti Umani. – 1. I diversi profili della vulnerabilità nell'era delle tecnologie digitali. – 2. Un particolare ambito della vulnerabilità tecnologica: le neurotecnologie. – 3. (segue) Le neurotecnologie: il quadro normativo di riferimento e le ricerche scientifiche sul punto. – 4. Incertezza normativa e proposte di soluzione in una prospettiva etica e giuridica – Conclusioni.

Introduzione. L'inquadramento giuridico della "vulnerabilità": le difficoltà di classificazione e l'apporto della Corte Europea dei Diritti Umani.

Il paradigma delle *vulnerabilità* si è affermato in maniera significativa in molteplici discipline, acquisendo in ciascuna area prospettive peculiari e varietà di significati[1].

Si tratta di una nozione mutevole la cui definizione può sfuggire o, al contrario, risultare semplicistica ad una prima e superficiale osservazione; ciò in quanto la vulnerabilità è idonea a ricomprendere molteplici e, soprattutto, diverse "figure soggettive"[2].

Da un punto di vista giuridico, la nozione di vulnerabilità è impiegata, con sempre maggiore frequenza, sia in provvedimenti giurisdizionali[3], sia in testi normativi[4].

Da questo punto di vista, rilevante è il contributo proveniente dalla Corte Europea dei Diritti Umani che, in molteplici sentenze, si riferisce alla nozione di vulnerabilità in relazione ad una esigenza di tutela adeguata dei soggetti che si trovano in situazioni di svantaggio, contribuendo a consolidare un'interpretazione dei principi convenzionali in una prospettiva antidiscriminatoria.

Nelle argomentazioni della Corte[5], in particolare, la vulnerabilità è intesa in una duplice accezione: come condizione di un gruppo che può essere

[1] Questo approccio è maturato nell'ambito del Progetto Jean Monnet Chair dal titolo ProTech (*European Protection of Individuals in relation to New Technologies* – prof. L. Gatt), disponibile al sito https://www.protech-jeanmonnet.eu, 2019 – 22.

[2] B. Pastore, *Semantica della vulnerabilità, soggetto, cultura giuridica*, 2021, 77. Sul punto anche A. Fusaro, *Il negozio della persona vulnerabile e il linguaggio delle invalidità*, in *Ars Interpretandi*, 2019, 39-63.

[3] E. Diciotti, *La vulnerabilità nelle sentenze della Corte Europea dei Diritti dell'Uomo*, in *Ars Interpretandi*, 2018, 13-34

[4] Sul punto M. Virgilio, *La vulnerabilità nelle fonti normative italiane e dell'Unione Europea: definizioni e contesti*, in O. Giolo e B. Pastore (a cura di), *Vulnerabilità. Analisi multidisciplinare di un concetto*, Roma, 2018, 161-170.

[5] L. Peroni, A. Timmer, *Vulerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law*, in *Internationale Journal of Costitutional Law*, 2013, 1056-1085; A. Timmer, *A quiet Revolution: Vulnerability in the European Court of Human Rights*, in M.A. Fineman and A. Grear (eds.), *Vulnerability. Reflections on a New Ethical Foundation for Law and Politics*, Ashgate, Farnham-Burlington, 2013, 147-170.

destinatario di comportamenti discriminatori – come nel caso dei disabili[6] - ma anche come attributo potenzialmente riferibile all'essere umano in quanto tale, come condizione universale.

L'elemento che, invece, accomuna le decisioni della Corte è la considerazione che la vulnerabilità debba essere considerata alla luce del caso concreto, in quanto categoria che opera in modo "relazionale"[7] e che, per tale motivo, è suscettibile di caratterizzarsi in modo diverso a seconda delle peculiarità della singola fattispecie.

Pur nell'eterogeneità che caratterizza le ipotesi cui la categoria della vulnerabilità si riferisce, dunque, ciò che rileva è la finalità unica di apprestare idonea protezione alle persone ed ai loro diritti.

La Corte non fornisce una definizione di vulnerabilità[8] ma la individua come categoria che si riferisce alle situazioni in cui i soggetti sono, in vario modo, condizionati nel loro agire in quanto parti di un rapporto sbilanciato, anche solo da un punto di vista informativo, che può caratterizzare tutti gli individui in quanto destinatari di potenziali lesioni riferibili a fattori diversi.

Ciò implica che la tutela per tali situazioni disomogenee non può essere unica ma debba calibrarsi a seconda delle peculiarità del caso concreto [9], fermo restando il fine ultimo di tutela della persona e della sua dignità[10].

1. I diversi profili della vulnerabilità nell'era delle tecnologie digitali.

La vulnerabilità intesa come condizione umana che caratterizza tutte le persone fisiche, riferibile non solo gli individui appartenenti a gruppi tipicamente connotati da un requisito di fragilità (minori, anziani, disabili) e ritenuti bisognosi di una maggior tutela da parte dell'ordinamento giuridico quanto, piuttosto, all'individuo in quanto tale in relazione al contesto in cui opera, sembra potersi riferire anche alle nuove fattispecie determinate dallo sviluppo delle tecnologie.

Si tratta, infatti, di una nozione di vulnerabilità che è idonea a ricomprendere anche quelle condizioni soggettive caratterizzate da squilibri dovuti non solo a condizioni di salute o all'età anagrafica.

In altre parole, le particolari caratteristiche del contesto digitale – inteso come il mondo virtuale di *internet* ma quello determinato dalle particolari interazioni di un soggetto con *devices* tecnologici anche non collegati alla rete – potrebbero consentire una graduazione della categoria della vulnerabilità tale da ricomprendere i riflessi negativi sulla capacità di autodeterminazione degli individui in varie fattispecie connotate dall'utilizzo di uno strumento tecnologico, che caratterizza e distingue la fattispecie in oggetto.

---

[6] Si tratta di decisioni che hanno contributo a fornire una interpretazione estensiva degli articoli 3 e 4 CEDU. Al riguardo, *Chapman c. Regno Unito* [GC], (27238/95), 18 gennaio 2001; con specifico rifermento ai disabili *Kudla c. Polonia* [GC] [30210/96], 26 ottobre 2000; *Renold c. Francia*, [5608/05], 16 ottobre 2008).

[7] Così B. PASTORE, *Semantica della vulnerabilità, soggetto, cultura giuridica*, cit., 79.

[8] R. CHENAL, *La definizione della nozione di vulnerabilità e la tutela dei diritti fondamentali*, in *Ars Interpretandi*, 2018, 35-55.

[9] D. POLETTI, *Soggetti deboli*, in *Enc. dir.*, VII, Milano, 2014, 962-986.

[10] F.D. BUSNELLI, *La dimensione della fragilità della persona umana fra principi e regole*, in F. FONTANA, A. TARANTINO (a cura di), *Dignità e fragilità della persona umana*, 2017, 27 ss.

In via di estrema generalizzazione, potrebbe essere utile distinguere al riguardo due possibili scenari relativi alla vulnerabilità in relazione al mondo digitale: in un primo caso, essa potrebbe riguardare il particolare operare nel contesto tecnologico di tutti quegli individui che non si distinguono per una precedente loro categorizzazione come soggetti fragili[11]. Si considerino al riguardo le asimmetrie informative così come i condizionamenti – anche indiretti – delle scelte dei soggetti che operano nella rete *internet*; ne costituisce valido esempio l'effetto distorsivo determinato dalla mancanza di trasparenza delle piattaforme per il commercio *online*[12].

Nel secondo caso, invece, potrebbe verificarsi una duplicazione della vulnerabilità nella misura in cui alla originaria condizione di fragilità determinata da un particolare stato fisico o mentale si aggiunga una ulteriore condizione di debolezza dovuta in questo caso all'interazione del singolo con strumenti tecnologici[13]. Si può pensare, in questa seconda ipotesi, alle conseguenze negative, dirette o indirette, derivanti dalla rete *internet* che, per vari fattori, possono incidere negativamente nella sfera giuridica dei minori, soggetti vulnerabili per definizione da sempre tutelati dall'ordinamento, anche di fonte europea[14]. Ma si può fare riferimento anche al particolare impatto che sul singolo può determinare l'impiego di applicazioni che, grazie alla tecnologia, sono state sviluppate per creare nuovi strumenti di inclusione per persone con menomazioni fisiche o psichiche ed, in quanto tali, impossibilitati ad interagire con altri consociati[15] o ad esplicare la loro capacità negoziale[16]. SI fa riferimento

[11] L. GATT, *The vulnerability of the human being in a technological environment: the need for protective regulation*, in *Social networks and multimedia habits*, Napoli, 2020, 7 ss.

[12] R. MONTINARO, *Online Platforms: new vulnerabilities to be addressed in the European framework. Platform to consumer relations*, in EJPLT, 2020, II, 53-64.

[13] Parla, in particolare, di "*vulnerabilità intersezionale*" per indicare la possibilità che in capo agli stessi soggetti si sommino più condizioni di vulnerabilità B. PASTORE, *Semantica della vulnerabilità, soggetto, cultura giuridica*, cit., 80.

[14] I. A. CAGGIANO, *Minori d'età e GDPR,* in Aa. Vv., *Diritto di Famiglia e nuove tecnologie,* (a cura di) E. DE BELVIS, 2021, 189 - 214; ID, *"Privacy" e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 2018. Consultabile al sito *http://www.ejplt.tatodpr.eu/Article/Archive/index_html?ida=24&idn=2&idi=-1&idu=-1*

[15] Grazie ad una ricerca condotta dall'Università della California, finanziata tra l'altro anche dal laboratorio di ricerca Facebook Reality Labs (FRL) afferente a Facebook, un uomo che aveva perso la parola a causa di un grave ictus è tornato a parlare dopo quindici anni, grazie ad un impianto che traduce i segnali cerebrali in codice decifrabile dal *computer* in tempo reale. Lo studio è stato pubblicato sul *New England Journal of Medicine* ed è disponibile qui https://www.nejm.org/doi/full/10.1056/NEJMoa2027540?query=featured_home

[16] Trib. Milano, 24 febbraio 2015, n. 11965/2011 in banca dati *Pluris*. Per la prima volta ad una persona malata di Sclerosi Laterale Amiotrofica (soggetto pienamente capace di agire, e quindi di testare, ma impossibilitato a parlare) viene riconosciuta la possibilità di esprimere le proprie volontà con testamento pubblico, innanzi ad un notaio. Decidere diversamente, precisa il giudice di merito, avrebbe determinato una ingiustificata discriminazione a causa della grave malattia debilitante del soggetto in questione. Si legge nella decisione che "*il paziente affetto da SLA possa fare testamento dettando le proprie volontà ad un amministratore di sostegno avvalendosi del comunicatore oculare, non potendosi ammettere che un individuo perda la capacità di testare a causa della propria malattia, trattandosi di una discriminazione fondata sulla disabilità, precisando inoltre che per i pazienti affetti da SLA deve ritenersi sussistente un vero e proprio diritto alla comunicazione non verbale, mediante un comunicatore a puntamento oculare*". Precedente analogo in Trib. Varese, 12 marzo 2012, in banca dati *Pluris*, con cui si è riconosciuta la possibilità per un soggetto malato di SLA incapace non solo di parlare ma anche di sottoscrivere, di esprimere le sue ultime volontà, questa volta nella forma del testamento olografo, ma sempre per il tramite di un puntatore oculare e di un curatore speciale nominato ad hoc (stante il conflitto di interesse dell'amministratore di sostegno nominato in quanto beneficiario di alcune disposizioni testamentarie) che ha provveduto a trascriverle. In questo secondo provvedimento, il Tribunale si dilunga ampiamente sulla capacità di testare di un soggetto che non può considerarsi giuridicamente incapace in considerazione della malattia che lo affligge, richiamandosi espressamente al

in questo caso all'ambito delle neurotecnologie.

2. Un particolare ambito della vulnerabilità tecnologica: le neurotecnologie.

Le neuroscienze si occupano di studiare il funzionamento del cervello umano, fornendo informazioni importantissime sui processi celebrali che sono di fondamentale importanza per la realizzazione di strumenti volti a migliorare i servizi di neuroriabilitazione e di salute mentale[17].

Più in particolare, i risultati delle indagini neuroscientifiche sono stati notevolmente potenziati grazie all'evoluzione tecnologica che ha consentito lo sviluppo di *devices* variamente impiegati nella cura di alcune patologie, anche neurodegenerative, che si caratterizzano per un diverso grado di invasività e che sono tali da non consentire unicamente un'attività di monitoraggio della mente umana ma anche di incidere su di essa fino al punto da alterarla in maniera considerevole.

Il riferimento in particolare è a quei dispositivi neurotecnologici che sono in grado di *fotografare* la mente umana grazie a tecniche di "*neuroimaging*"[18] come l'encefalografia (EEG) o la risonanza magnetica funzionale (fMRI) che sono state definite tecniche di "*brain reading*"[19] per la loro capacità di cogliere stati mentali inespressi e stati inconsci dei soggetti sottoposti a tali tecniche[20].

Sono del pari strumenti neurotecnologici quei *devices* che sfruttano l'attività elettrica rilevabile dal cuoio capelluto e che si distinguono in tre categorie a seconda del diverso livello di invasività che possono avere sul soggetto.

Un primo gruppo di dispositivi consentono di controllare un *computer* usando segnali celebrali generati dal cervello, da segnali muscolari o dal movimento oculare.

Si tratta delle c.d. "*interfacce uomo-macchina*" che consentono a persone con forte disabilità motoria di controllare strumenti come una sedia a rotelle motorizzata o una tastiera virtuale con i soli occhi.

Le "*interfacce cervello-macchina*", invece si caratterizzano per il rilevamento unicamente di segnali celebrali. Possono al riguardo distinguersi i dispositivi che consentono di instaurare, tramite la tecnica di "*Brain Computer Interface*" (BCI)[21], un percorso di comunicazione diretto tra il cervello e dispositivi esterni e, dunque, volti unicamente a raccogliere dati; nonché dispositivi che consentono anche di inviare impulsi al cervello con le tecniche di "*Deep Brain*

---

riguardo la Convenzione di New York del 13 dicembre 2006, sui diritti delle persone con disabilità, ratificata dall'Italia con legge del 3 marzo 2009, n. 18 che riconosce "*l'importanza per le persone con disabilità della loro autonomia ed indipendenza individuale, compresa la libertà di compiere le proprie scelte*"

[17] Parla di "era Neurocentrica", per indicare la centralità degli studi neuroscientifici anche rispetto alle scelte di governative e politiche in generale J.F. DUNAGAN, *Politics for Neurocentric Age*, *in Journal of Futures Studies*, 2010, 51-70.

[18] K. O'CONNEL, *From Black Box to 'Open' Brain. Law, neuroimaging and disability discrimination*, in *Griffith Law Review*, 2011. 883-904.

[19] J.D. HAYNES, *Brain Reading: decoding mental states from brain activity in humans*, in *The Oxforz Handbook of Neuroethics*, 2011, 3 ss.

[20] M. BLES, J.D. HAYNES, *Detecting concealed information using brainimaging technology*, in *Neurocase*, 2008, 82 ss; S. BODE, AH. HE, CS. SOON, R. TRAMPEL, R. TURNER, J.D. HAYNES, *Tracking the unconscious generation of free decisions using ultra-hight field fMRI*, in *PloS one*, 2011

[21] Con specifico riferimento all'impiego di tali tecniche al di fuori dell'ambito medicale M.D. TENNISON, J.D. MORENO, *Neuroscience, Ethics and National Security: the state of the art*, in *PLoS Biology*, 2012.

Stimulation" (DBS) [22] attraverso la somministrazione di impulsi elettrici in piccole aree del cervello mediante elettrodi impiantati sul paziente[23].

Alcuni di questi strumenti esistono già da molto tempo, non sono quindi il risultato dell'evoluzione tecnologica in tale ambito.

Ciò che costituisce un elemento di novità è, invece, l'uso crescente dell'intelligenza artificiale - si pensi alle tecniche di "*machine learning*" a "*deep learning*" - che ha notevolmente potenziato i dispositivi neurotecnologici che, tramite l'utilizzo di algoritmi sofisticati, possono essere anche *closed loop*, ovvero bidirezionali e quindi in grado non solo di raccogliere segnali ma anche di inviare impulsi verso specifiche aree celebrali, così da automatizzare il processo decisionale e da raccogliere i dati generati da queste tecnologie.

Pertanto, la rilevanza da un punto di vista giuridico delle neurotecnologie è riferibile alla loro capacità di leggere il cervello umano e di indirizzarlo o condizionarlo a seconda delle ipotesi[24]. Più in particolare, si tratta di un duplice livello di analisi, attinente il primo alla tutela dell'identità e capacità di autodeterminazione degli individui[25]; il secondo relativo alla tutela della *privacy* e riservatezza personale.

Occorre, dunque, osservare come la possibilità di incidere sull'attività celebrale di una persona comporti il rischio di una alterazione incontrollata della sua identità, ciò in una duplice accezione: sia come possibilità di non riuscire ad identificare un soggetto in quanto tale, laddove non si riesca più a distinguere la sua autonoma attività celebrale rispetto a quella indotta da dispositivi esterni; sia come alterazione della sua capacità di autodeterminarsi in maniera libera, compiendo scelte e ponendo in essere atti rilevanti senza alcun condizionamento.

Se il soggetto sottoposto alle tecniche di BCI o DBS non riesce a mantenere il controllo dei propri movimenti e comportamenti, ciò incide inevitabilmente sulla sua autonomia e, dunque, rende difficile l'imputazione a se stesso degli atti compiuti, con conseguente alterazione del relativo regime di responsabilità[26].

In tal modo, l'identità personale del soggetto sottoposto a tali tecniche resta celata, messa in qualche modo in secondo piano, ciò nella misura in cui non sia più possibile distinguere nettamente il soggetto agente. Vi è, dunque, in queste ipotesi un problema di *mental integrity*[27] di non poco conto.

Dal punto di vista della tutela dei dati personali, invece, i rischi sollevati

---

[22] S. Desmoulin-Canselier, *Ethical and Legal Issues in Deep Brain Stimulation: An Overview*, in *Neuroscience and Law*, 2021, 319 ss.

[23] Si tratta di tecniche impiegate per la cura di malattie neurodegenerative come il parkinson, ma anche epilessia, disturbi del movimento ed altre patologie psichici. L'invasività di tali tecniche è tale da necessitare l'impianto di elettrodi nel torace che comportano una stimolazione celebrale che in alcuni casi può essere controllata dal paziente (dispositivi *open-loop DBS*) mentre, di più recente emersione, quelli che si basano su controllo automatico operato da un algoritmo (*dispositivo closed-loop DBS*)

[24] P.R. Roelfsema, D. Denys, P.C. Klink, *Mind Reading and Writing: the future of Neurotechnology*, in *Trends in Cognitive Sciences*, 2018, 598-610.

[25] L. Tafaro, *Some Reflections on Neuroscience and Civil Law*, in *Neuroscience and Law*, 2021, 113 ss.

[26] Con specifico riferimento alla responsabilità penale O.R. Goodenough, M. Tucker, *Why Neuroscience Matters for Law*, in *Neuroscience and Law*, 2021, 51 ss.

[27] S. Fuselli, *Neurotecnologie e tutela dell'integrità psichica. Profili filosofico-giuridici di un mutamento in atto, in Journal of Ethics and Legal Technologies*, 2020, 15, il quale riprende la definizione di A. Lavazza, *Freedom of Thought and Mental Integrity: the moral requirements for any neural prosthesis*, in *Frontiers in neuroscience*, 2018, 82.

dagli strumenti sopra descritti sono rilevanti in quanto potenzialmente idonei a cogliere, oltre che a divulgare, informazioni dettagliate sullo stato mentale di una persona [28] che diversamente resterebbero inespresse perché non comunicabili dal soggetto interessato né in maniera palese (attraverso le parole o lo scritto) né tacita (attraverso un dato comportamento) ed idonei a prevedere il comportamento del soggetto. Si sviluppano, in tal modo, nuovi metodi di trattamento dei dati personali che sono in grado di configurare veri e propri "profili predittivi".

3. *(segue)* Le neurotecnologie: il quadro normativo di riferimento e le ricerche scientifiche sul punto.

L'accelerazione della trasformazione digitale e l'utilizzo delle tecnologie dell'informazione e della comunicazione (TIC), dell'intelligenza artificiale e della robotica favorisce la progettazione di servizi per le esigenze specifiche delle persone disabili colmando il vuoto di tutela creato dai servizi di sostegno tradizionali.

Il campo delle neuroscienze e delle neurotecnologie, in particolare, favorisce l'autonomia dei singoli, delle famiglie e delle persone che se ne prendono cura, eliminando le barriere create dalla disabilità.

Da un punto di vista normativo, i diritti delle persone disabili ricevono esplicito riconoscimento quali diritti fondamentali con la Convenzione Onu sui diritti delle persone con disabilità (UNCRPD) che valorizza la diversità nonché l'autonomia ed autodeterminazione delle persone disabili. Principi che, tuttavia, benché non espressi, erano già sottesi alla Convenzione Europea dei diritti dell'uomo e confermati dalla Carta europea dei diritti dell'uomo.

L'Unione europea si fonda sui valori della dignità umana, dell'uguaglianza, del rispetto dei diritti umani, compresi i diritti delle persone con disabilità. Al fine di dare concreta attuazione alla Convenzione delle Nazioni Unite sui diritti delle persone con disabilità (art. 3, comma 1, lettera "d") e alla Carta dei diritti fondamentali dell'UE, dunque, nel mese di marzo 2021 la Commissione Europea ha adottato la Strategia per i diritti delle persone con disabilità 2021-2030 che, riprendendo i risultati della precedente strategia europea sulla disabilità 2010-2020, ha l'obiettivo di aumentare il livello di autonomia delle persone disabili, favorendone l'inclusione e promuovendo un principio di uguaglianza in linea con l'articolo 1 della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità (UNCRPD),

Al fine di promuovere il progresso scientifico e tecnologico, negli ultimi anni sono stati adottati diversi atti legislativi e raccomandazioni per consentire la tutela dei soggetti che si trovano in una posizione di debolezza rispetto ad altri, ciò anche in ambiente digitale.

Al riguardo, dapprima la direttiva 2016/2102/UE, c.d. *Web Accessibility Directive*, ha avuto l'obiettivo di garantire l'accessibilità alle tecnologie e ai sistemi di informazione e comunicazione anche alle persone disabili; successivamente il c.d. *European Accessibility Act*, confluito in parte nella

[28] Si tratta del c.d. "processo di inferenza inversa" M. IENCA, *Neurodiritti: storia di un concetto e scenari futuri*, Atti del Convegno "Privacy *e neurodiritti. La persona al tempo delle neuroscienze*, 2021, 39.

direttiva UE 2019/882 del parlamento europeo e del consiglio del 17 aprile 2019, si propone di rimuovere gli ostacoli all'accessibilità anche nel campo delle tecnologie dell'informazione e della comunicazione.

Con particolare riferimento poi alle neuroscienze, in concreto sono molti i progetti europei che sono stati avviati nell'ambito dello studio del funzionamento del cervello umano. Il più importante tra questi è il progetto "*Human Brain Project*" il cui scopo è quello di costruire una piattaforma tecnologica *online*, solo per le neuroscienze, la medicina, le tecnologie dell'informazione e della comunicazione (ICT).

A questo si affiancano altre iniziative, tutte accomunate dall'intento di sfruttare la potenza delle tecnologie digitali ed il peso crescente dell'informatica per potenziare la ricerca in relazione alle neuroscienze cognitive e dei progressi TIC ispirati al cervello. Le motivazioni che sono alla base di queste ricerche partono dalla considerazione che i progressi tecnologici possano aiutare i pazienti affetti da disabilità gravi a gestire meglio le proprie condizioni, portando così a miglioramenti nella qualità della vita, come nel caso della c.d. "tecnologia indossabile"[29].

Tuttavia, non si rinviene allo stato uno specifico riferimento normativo per la tutela dei particolari stati soggettivi connessi all'impiego di dispositivi tecnologici nel campo delle neuroscienze rispetto agli ambiti innanzi analizzati.

Ciò ha dato luogo ad un ampio dibattito circa la possibilità di limitarsi ad interpretare estensivamente le norme già esistenti oppure, al contrario, di prendere in considerazione la specificità delle fattispecie determinate dall'impiego di strumenti neurotecnologici e pensare, così, all'introduzione di diritti nuovi, in funzione di tutela della particolare condizione di vulnerabilità del paziente sottoposto a tecniche di BCI o DBS e, più in generale, alle interfacce uomo-macchina che incidono sull'attività celebrale, alterandola e modificandola.

In particolare, non vi è certezza che l'art. 3 della Convenzione dei Diritti Fondamentali dell'Unione europea che disciplina il diritto all'integrità psichica possa ricomprendere anche la tutela delle possibili alterazioni del processo celebrale determinato dalle neurotecnologie[30].

Al riguardo, un primo approccio al tema suggerisce di operare una interpretazione evolutiva e tecnologicamente orientata non solo della norma innanzi citata, ma anche degli articoli 7 e 9 della Convenzione, nonché dell'art. 22 GDPR in relazione alla decisione algoritmica[31].

Secondo una diversa ricostruzione della fattispecie, invece, non sarebbe

---

[29] Si considerino i seguenti progetti di ricerca: "AETINOMY" (https://cordis.europa.eu/article/id/308439-a-digital-disease-classification-system-fit-for-the-modern-medical-era/it) che analizza mediante algoritmi causa ed effetti delle malattie neurodegenerative; NOSUDEP (https://cordis.europa.eu/article/id/308443-wearable-devices-to-help-prevent-sudden-unexpected-death-through-epilepsy/it) che si basa sulla elettronica indossabile come mezzo per aiutare le persone affette da epilessia; BREAKBEN (https://cordis.europa.eu/article/id/308440-breaking-through-barriers-for-a-revolution-in-brain-scans/it) sulla ricerca delle scansioni celebrali con magnetometri altamente sensibili; PRONIA (https://cordis.europa.eu/article/id/239895-novel-algorithms-can-predict-psychosis-before-it-strikes/it) che ha creato algoritmi per previsioni precise delle psicosi.

[30] S. Fuselli, *Neurotecnologie e tutela dell'integrità psichica. Profili filosofico-giuridici di un mutamento in atto*, cit., 11

[31] O. Pollicino, *Costituzionalismo,* privacy *e neurodiritti*, Atti del Convegno "Privacy *e neurodiritti. La persona al tempo delle neuroscienze*, 2021, 79.

sufficiente il richiamo alle norme già esistenti ma occorrerebbe introdurre una nuova categoria di diritti cui si dà il nome di *neurorights.*

È stata, infatti, avanzata la proposta di introdurre norme che tutelino diritti nuovi come la *privacy mentale*, intesa come il diritto ad evitare l'accesso non autorizzato alle informazioni personali inespresse, evitando il rischio di perdita di controllo dei dati da parte del paziente con conseguente rischio che gli stessi siano accidentalmente o illecitamente divulgati; *il diritto alla continuità psicologica* per evitare manipolazioni dell'attività celebrale che vadano ad incidere sull'identità personale dell'individuo; *il diritto alla libertà cognitiva*[32], ovvero alla possibilità di decidere autonomamente se sottoporsi o meno alle tecniche neuroscientifiche o di interromperne l'utilizzo[33].

Altra proposta è quella di adottare una "Dichiarazione Universale su Neuroscienze e Diritti Umani" al fine di adottare principi giuridici e valori condivisi a livello internazionale[34].

Si consideri, inoltre, al riguardo che considerazioni sul tema sono state fatte anche dal legislatore.

Il Cile è, infatti, il primo Paese al mondo ad essersi occupato, da un punto di vista legislativo e regolamentare, dei rischi connessi alle neurotecnologie, come la perdita della *privacy mentale*.

Sono ben due, infatti, i progetti di legge al riguardo: con il primo si propone un emendamento alla Costituzione per definire, per la prima volta, l'identità mentale come un diritto, da tutelare in via regolamentare e non disponibile né manipolabile da parte di alcuno, neppure per motivi di salute; il secondo progetto di legge, (già approvato in Senato) invece, che mira a regolamentare le neurotecnologie, al fine di protegge i diritti all'identità personale, al libero arbitrio, alla *privacy* mentale, all'accesso equo alle tecnologie che aumentano le capacità umane e il diritto alla protezione contro pregiudizi e discriminazioni.

Il presupposto di tali iniziative legislative è rappresentato da un nuovo e diverso concetto di *privacy* che si concentra sui dati neurali e sulle informazioni riguardanti i nostri processi e stati mentali che possono essere ottenute analizzandoli, con l'obiettivo di considerare tali dati neurali alla stregua di un tessuto organico, che in quanto tali non possono essere oggetto di atti di disposizione a titolo oneroso, ma soltanto donati per scopi altruistici.

Con particolare riferimento alla ricerca scientifica sul punto, inoltre, il gruppo di ricerca della Columbia University degli Stati Uniti, coordinato dal Prof. Rafael Yuste, che si occupa delle più avanzate tecniche di "*brain reading*" ha auspicato l'inserimento dei neurodiritti nei trattati internazionali e, più in

---

[32] In riferimento al significato di libertà cognitiva in relazione ai diritti umani e di come tale relazione possa cambiare in ragione delle scelte legislative P. SOMMAGGIO, M. MAZZOCCA, *Cognitive Liberty and Human Rights*, in *Neuroscience and Law*, 2021, 95 ss.

[33] M. IENCA, *Tra cervelli e macchine: riflessioni su neurotecnologie e su neurodiritti*, in *Notizie di POLITEIA*, XXXV, 133, 2019, 52-62, in quale aveva già teorizzato l'introduzione di un diritto alla *privacy* mentale in M. IENCA, R. ADORNO, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sciences, Society and Policy*, 2017, 5 i quali hanno anche avviato una raccolta firme per l'introduzione di una *"Neuro - specific human rights Bill"* ovvero una Carta dei neurodiritti, visionabile al seguente link http://www.globalneuroethics.com.

[34] F.G. PIZZETTI, *Brain- Computer Interfaces and the Protection of the Fundamental Rights of the Vulnerable Persons*, in *Neuroscience and Law*, 2021, 291 ss.

particolare, della Dichiarazione Universale dei Diritti Umani[35].

Anche il Comitato internazionale di bioetica dell'Unesco si sta occupando delle sfide etiche connesse alla neurotecnologie[36], mentre il Consiglio d'Europa ha approvato il *"Piano strategico sui diritti umani e le tecnologie in biomedicina (2020-2015)*" che prevede come obiettivo, tra gli altri, proprio l'accertamento dell'adeguatezza dell'attuale quadro normativo rispetto alla tutela dei diritti umani con specifico riferimento alle neurotecnologie[37].

4. Incertezza normativa e proposte di soluzione in una prospettiva etica e giuridica.

Il complesso quadro normativo e di ricerca scientifica in tema di neuroscienze e neurotecnologie innanzi analizzato mette in evidenza come il tema della vulnerabilità tecnologica in tali ambiti sia di estrema rilevanza in una prospettiva giuridica, oltre che etica[38], laddove si considerino i possibili impatti negativi della tecnologia sui diritti fondamentali di coloro che, per pregresse patologie fisiche o psichiche, siano già considerati dall'ordinamento giuridico soggetti vulnerabili.

E' possibile, dunque, rilevare l'ambivalenza del rapporto tra le nuove tecnologie e le particolari situazioni di vulnerabilità già esistenti.

Se da un lato, infatti, la tecnologia può in tali ambiti determinare un miglioramento della qualità della vita, nella misura in cui è possibile restituire alle persone interessate un certo livello di autonomia intesa come autosufficienza nel comportamento e nelle azioni che sono necessarie ai bisogni fisici e relazionali che consentono al soggetto un adeguato livello di inclusione sociale, dall'altro la nozione di autonomia intesa come diritto ad autodeterminarsi liberamente da sé nel pensiero e nell'azione rischia di essere seriamente compromessa.

In relazione a tale dato fattuale, non può non considerarsi come il dibattito intorno alla possibilità che si riconoscano nuovi diritti a tutela delle situazioni soggettive relative alle neurotecnologie può rappresentare un primo tentativo di porre l'attenzione su fattispecie che l'evoluzione tecnologica ha determinato e che non possono non essere prese in considerazione da un punto di vista sia etico che giuridico.

Tuttavia, l'introduzione di specifiche norme volte a tutelare i c.d. *neurorights* potrebbe risultare intervento parziale se ciò non si accompagni ad un mutamento dell'approccio ai sistemi di regolamentazione delle nuove tecnologie.

Limitarsi ad interventi *ex post* in funzione rimediale delle possibili lesioni che la tecnologia può determinare rispetto ai diritti fondamentali delle persone

---

[35] http://www.humanrightscolumbia.org/events/neurorights-human-rights-guidelines-neurotechnology-and-ai ; S. GOERING, R. YUSTE, *On the Necessity of Ethical Guidelines for Novel Neurotechnologies*, in *Cell 167*, 2016, 882 ss.

[36] http://www.unesco.it/it/TemiInEvidenza/Detail/17

[37] https://unipd-centrodirittiumani.it/public/docs/Strategic_Action_Plan_Final_Epdf.pdf

[38] K.H. KESKINBORA, K. KESKINBORA, *Ethical considerations on novel neuronal interfaces*, in *Neurological Sciences*, 2018; R. STRAND, M. KAISAR, *Report on Ethical Issues Raised by Emerging Sciences and Technologies*, Norway, 2015, 12ss.

non appare soluzione adeguata alla complessità delle situazioni giuridiche che caratterizzano tali ambiti e che rischiano di non trovare adeguata tutela nel caso concreto.

Come precisato dalla Corte Europea dei Diritti Umani, infatti, la vulnerabilità è una condizione che richiede una tutela calibrata sulle specificità del caso concreto in quanto l'eterogeneità delle situazioni coinvolte non consente di adottare un unico e conformato strumento di protezione.

Ciò è particolarmente rilevante in relazione alle situazioni di vulnerabilità relative alle neurotecnologie che induce a ritenere che l'impatto che si determina sui diritti fondamentali delle persone debba essere valutato preventivamente rispetto alla produzione di dispositivi tecnologici.

Ciò che manca, dunque, non è tanto una risposta sul piano legislativo – che da sola rischia di risultare inadeguata – quanto un intervento specifico del giurista esperto in tali ambiti nella fase precedente – e non successiva – rispetto all'immissione sul mercato di prodotti che, se non adeguatamente valutati anche da un punto di vista giuridico e non solo delle funzionalità tecniche, rischiano di incidere sulle categorie giuridiche fondamentali e sui diritti delle persone.

Occorrerebbe, dunque, al riguardo una riflessione giuridica integrata nella sperimentazione bio-ingegneristica in cui il *design* dei prototipi, prodotti o servizi tecnologici sia ispirato a *standard* minimi, etici e giuridici, cui le principali aziende tecnologiche devono attenersi per realizzare prodotti rispondenti all'impianto normativo, già esistente o che potrebbe essere approvato al riguardo.

Ciò che deve essere favorito, pertanto, è uno sviluppo tecnologico *human-centered*, volto a ridurre la disabilità ma allo stesso tempo orientato ad una prospettiva etico-giuridica grazie alla collaborazione del giurista con le aziende produttrici che, intervenendo nella fase della progettazione dei dispositivi, possa valutare l'impatto della tecnologia prima che questa venga diffusa.

Il diritto all'autodeterminazione nel pensiero e nell'azione, lungi dal costituire un argine all'evoluzione tecnologica, deve essere sotteso ad ogni forma di progresso e fungere da faro, per evitare che la disabilità divenga un mezzo per incidere sulle categorie giuridiche della volontà e della capacità dei soggetti. Ciò sul presupposto che l'autonomia del singolo sia inevitabilmente collegata alla sua identità.

Tale prospettiva implica necessariamente una stretta collaborazione tra il giurista, da un lato, ed altre professionalità con differenti *background* scientifici, oltre che operatori del settore privato, sul presupposto che la multidisciplinarietà nell'analisi di una fattispecie possa innescare un mutamento nella percezione della sua esatta natura[39], grazie agli apporti provenienti dai diversi esperti coinvolti nell'attività di progettazione di prototipi tecnologici.

Ciò che deve rappresentare il *trait d'union* delle diverse competenze coinvolte nella fase di progettazione è un particolare approccio alla vulnerabilità, in cui il centro dell'attenzione è la persona nella realtà vissuta della malattia, ove si mettano in luce la molteplicità degli aspetti coinvolti, non

[39] G. Pascuzzi, *Quale formazione per la ricerca interdisciplinare?,* in *BioLaw Journal – Rivista di BioDiritto*, 2021, 337-343.

solo giuridici e tecnici ma anche etici, morali, culturali. Ciò al fine di creare dei veri e propri *Spazi Etici*[40] nella programmazione di prodotti tecnologici che tengano conto della complessità ed eterogeneità degli interessi coinvolti.

Conclusioni.

Appare considerazione pacifica che la tecnologia possa rappresentare il principale ausilio delle persone vulnerabili – a causa di varie forme di disabilità - per ridurre le distanze sociali e vivere in modo libero e autonomo, grazie ai dispositivi che consentono il recupero di capacità fisiche e psichiche.

Tuttavia, lo sviluppo tecnologico deve necessariamente essere ispirato al principio della libera autodeterminazione dell'individuo, per evitare un possibile "abuso della tecnica" a discapito del progresso e dei vantaggi che esso può determinare per le persone disabili.

La tecnologia, in altre parole, non può essere causa, a sua volta, di un ulteriore profilo di vulnerabilità che, tuttavia, rischia di non trovare una compiuta tutela laddove non si intervenga già nella fase di progettazione.

Occorrerebbe, dunque, un potenziamento del ruolo del giurista in tali ambiti, il quale non dovrebbe limitarsi a collaborare con le aziende tecnologiche redigendo modulistica di vario tipo, ma dovrebbe prendere parte ad una necessaria fase prodromica alla stessa progettazione, focalizzata sull'analisi comportamentale con l'obiettivo di cogliere le interazioni tra soggetto vulnerabile e dispositivo tecnologico.

In conclusione, la vulnerabilità tecnologica è fonte di specifiche esigenze di tutela che richiedono un intervento a più livelli, non solo legislativo ma anche di prassi applicative che devono essere orientate da una comprensione del livello di consapevolezza dell'impatto che le tecnologie possono determinare in capo ai singoli al fine di predisporre adeguate tutele rapportate, dunque, al caso concreto.

Una consapevolezza che per ispirare scelte eticamente qualificate deve necessariamente essere "misurata" in via preventiva e costituire il punto di partenza della progettazione di prodotti neurotecnologici.

[40] L. BATTAGLIA, L. GATT, A, MORRESI, P. GRIMALDI, *Lo spazio etico per i Minori nei Tribunali*, 202, in corso di pubblicazione.

SECTION II

FOCUS PAPERS

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Bigger is always not better; less is more, sometimes: the concept of data minimization in the context of Big Data.

MD. ABDUL MALEK*
Judicial Officer at Bangladesh Judicial Service

Abstract

With the data landscape of the universe expanding every second every day by leaps and bound, the data value also increases unprecedentedly. Particularly, the disruptive use of data in location tracking, predictive policing, fraud detection, healthcare, advertising media, and entertainment has already revitalized personal data in many ways. But massive amassing of data also gives rise to new issues regarding the Big Data effects, including privacy invasion, data breaches, and cyber threats, etc. Taking effective efforts for mitigating the risks of data explosion thus becomes indispensable for companies, organizations, and societies alike. In such background, this paper attempts to focus on the ways how the data minimization approach mitigates such risks and how this approach as a concept is being incorporated in legal instruments globally. After exploring practical methods of applying data minimization, the paper concludes by delineating the way out of the current dilemmas so created in the face of Big Data.

Keywords: Big Data; Data Minimization; Data Protection Law.

Introduction.

The cloud is being fed an enormous amount of data every second. About 2.5 quintillion bytes of data are produced by over 4.1 billion internet users every day. Every day, 95 million photos and videos are shared on Instagram, 306.4 billion emails are sent, and 5 million Tweets are made (Jacquelyn Bulao, 2020). Even, over 350 million photos are uploaded to Facebook each day (Internet World Stats, 2015). By the end of 2020, 44 zettabytes will make up the entire-digital universe. Here is not the end. About 463 exabytes of data will be generated each day by humans as of 2025 (Jacquelyn Bulao, 2020). Right now, although 58.7% of people around the world have access to the internet (ITU, 2015), it will be considerably augmented in the coming days. Hence, it is not unassuming that as our personal data becomes vast, valuable, and sensitive in the world of big data, our privacy concerns and data protection challenges are (and will be) undergoing more intricate situations due to the more advancement of numerous disruptive technologies in the real world.

Basically, the impact of Big Data robustly challenges the data protection regime, and the laws relevant in the field are also fighting for adequately reacting to such deep concerns and challenges. To exemplify them with some questions- if you are not doing hazardous work, should your employer ask for your blood group? When you are in the doctor's chamber for a medical service, should the doctor ask for your religion or ethnicity? Can your recruiter ask for details of health conditions if you are not applying for a manual job? 'In addressing issues akin to these questions in the data ocean, it is the data minimization concept that can help you to stand out. Being a core privacy principle and standard procedure, the concept of data minimization in fact arises as "a solution to the mitigating risks of data Tsunami" (Malek, 2020). This concept is thus being celebrated in the age of Big Data.

As aforesaid, while Big Data promises significant economic and social benefits, it also raises serious privacy concerns and sparks serious debate on its biased, opaque, and discriminating effects. Moreover, data breaches have evidently in recent years grown in number, scope, and magnitude, as it is aptly argued that, "most likely because of the increasing value of digital data about individuals and companies, and the increasing concentration of this data into big-data storage in databases" (Kirtley and Shally-Jensen, 2019). Accordingly,

*Md. Abdul Malek (LLM, Dhaka) works as a career judge at Bangladesh Judicial Service. At the time of publication, the author was working as Judicial Magistrate. He embarked on his professional journey with the Bangladesh Telecommunication Regulatory Commission, the country's national digital space controlling body.

since Big Data has paradoxes: perils alongside its potential, recognizing such paradoxes will help us understand this revolution better (see Richards & King, 2013). Being so is the fact; the problems concerning Big Data management attract some practical approaches or values in the implementation of the data minimization concept.

In such situations, this paper will focus on the imports of the concepts of Big Data and data minimization; and then on how and why the data minimization concept still has the potentials to mitigate the risks. It also highlights the significant jurisdictions of the contemporary globe that has already incorporated the data minimization approach in their legal instruments; and then suggests practical approaches regarding how to benefit from applying the concept in digital space. This paper also concludes by exploring the way out of the current dilemmas that result from data explosion and data minimization.

1. The Concept of "Big Data".

The concept of Big Data is a composite of many concepts (see Brady, 2019). It is rapidly evolving as buzzwords of the moment and one of the most hyped-up terms in recent years. Big Data simply means massive data collection from multiple sources. The term basically "refers to novel ways in which organizations, including government and businesses, combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising correlations" (Rubinstein, 2013). In fact, Big Data is a more powerful form of data mining that relies on huge volumes of data, faster computers and also involves, at its core, new analytic techniques to discover hidden and surprising correlations based on artificial intelligence and machine learning to mine the vast amount of at ever-increasing rates; and is being used to inform decisions that affect individuals.

Portraying in a different fashion, Big Data is a methodology rather than a particular selection device. Its' objective is to find 'small patterns' or 'correlations' that reveal new insights or truths. It thus represents a new frontier in how data is processed and used to inform decision-making. It also involves new analytic techniques to discover hidden and surprising correlations based on artificial intelligence and machine learning to mine the vast amount of at ever-increasing rates; it is also being used to inform decisions that have the potentials to affect individuals.

To demystify, it is opportune to posit at the outset that what is 'big' in Big Data is not necessarily the size of the databases, it's the big number of data sources. Big Data is not all about volume; it is big because "the large volume of the real-time data is stored from a variety of sources with random sampling, processed, and produced, in the way of data fusion to create complete-automated-insights" (Steward and Cavazos, 2019). Furthermore, it can be simplified that information becomes Big Data when the volume can no longer be managed with normal database tools. In fact, the concept of Big Data with the power of the machine learning technique is now better known

for its' identifying characteristics 5Vs, i.e., volume (large quantity), veracity (real-time data), velocity (speed), variety (data fusion), and value (worth). Therefore, the right definition of Big Data should in fact be: "Mixed Data" (see Dutcher, 2014; Steward and Cavazos, 2019).

As Kirtley and Shally-Jensen (2019) aptly opined that "the actual or quantifiable measurements of Big Data are still not yet known", it can then be summed up by adding that what is Big Data is hence the 'digital footprint' we intentionally or unintentionally leave behind with every digital step we take. Hence, in the light of the aforesaid dispositions, it can be understood as that it is big, not in terms of its size; instead, it is big because the large volume of the real-time data is stored from a variety of sources with random sampling, processed, and produced, in the way of data fusion to create complete-automated-insights. To clarify further, Big Data is an elaboration of data analysis. Data analysis generates reports on, for example, sales by month. Big Data analysis also examines sales but seeks to find patterns for the effect of time on a day consumers shop, the weather, location of the store, type of credit card, bundle of goods bought, and so on (see Steward and Cavazos, 2019).

Sources of Big Data are all around us and can roughly be divided into business data, human data, and machine data from the internet of things. Big Data examples include credit card transactions, health insurance claims, and online behavior, among others. It now "encompasses a much wider swath of enterprises, and thereby in aid of algorithm improves decision making, enhance efficiency, and, even, increase productivity" (Brynjolfsson, Hitt and Kim, 2011). Indeed, there is evidence that Big Data has led to major breakthroughs in healthcare, more efficient delivery of electrical power, reductions in traffic congestion, and vast improvements in supply chain management (see Tene and Polonetsky, 2013; (Rubinstein, 2013).

Actually, it is the case that "different individuals and organizations access Big Data for different purposes. This, in part, explains why multiple definitions arise in discussions and analyses on the topic" (Kirtley and Shally-Jensen, 2019, p.130). However, while Big Data promises significant economic and social benefits, it also raises serious privacy concerns and sparks serious debate on its biased, opaque, and discriminating effects. Surprisingly, when Big Data is applied in the legal context, as the law has sensitivity, it seriously raises deep concerns and sparks fierce debates for their social, legal, and ethical implications.

2. The Concept of Data Minimization.

Data minimization means the collection and retention of the minimum data possible. It is an "idea that one should only collect and retain that personal data which is necessary" (The International Association of Privacy Professionals, n.d.). The data minimization concept is thus one of the general principles of data protection, which "ideally suggests that the amount of data collected should be the minimal amount of data necessary to conduct businesses" (Kirtley and Shally-Jensen, 2019, p.130). It also refers to measures

performed by organizations to limit the personal data they collect from individuals. In addition to limiting upfront collection, "data minimization also involves deleting or erasing data that is no longer useful as well as setting age limits for data retention" (Dataguise, n.d.).

The concept is basically a concept generally mentioned in the context of protection of personal data, the meaning of which entails the process of gathering solely the data required for fulfilling a particular purpose; that is to say, organizations must only collect the minimum amount of data necessary to accomplish their business purposes; and process personal information that they actually need to achieve the objective of processing the data. It is thus such a principle stating that "data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy" (Experian, n.d.). The concept thus posits the practice of limiting the collection and retention of personal data, and only the minimum amount of data processing is permissible as much as required to carry out the stated purpose (see Tortoise & Hare, 2018) or necessary to accomplish a specified purpose.

The concept also represents best practices with maintaining customer trust and reducing the risk of unauthorized access and other security threats. As a core privacy principle relating to personal data protection law, it envisages that information about an identified or identifiable person can be permissible to process only legitimate processing of personal data. For example, gender may be more relevant than religion or ethnicity if it is for a medical service.

Instead of the 'save everything approach', embracing a data minimization policy as a core principle generally mentioned in the context of protection of personal data is to be prioritized, and unnecessary data is to be discarded, keeping only what is relevant and necessary (see Malek, 2020). Further, that data should be retained only as long as necessary or required by laws or regulations. Organizations or service providers need to ensure that you are not collecting more information than necessary or required. For example, if you only need the e-mail and name of a person to access a service, trying to obtain more information, such as their address or credit card information, is a violation of the General Data Protection Regulation, 2018.

3. Data Minimization Concept in Legal Instruments.

The data minimization concept is notably incorporated in the 2018 General Data Protection Regulation (GDPR), Articles 5, 25, 47, and 89. As one of the seven basic data protection principles under EU data protection law, the very concept lies at the heart of the law embodying as the spirit of the regulatory framework [GDPR, Chapter 2, Article 5 (1) (c)]. According to this regulation, personal data shall be 'adequate, relevant and limited' to what is 'necessary' in relation to the 'purposes' for which they are processed (data minimization) (Art. 5 GDPR, 2018).[1]

[1]Art. 5 (1)c of the GDPR, 2018- "Principles Relating to Processing of Personal Data": adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') <https://gdpr-text.com/read/article-5/> accessed Summer 1, 2021

Although the term ‘data minimization’ is used multiple times in the GDPR, it does not define “adequate, relevant and limited”, but simply states that “the assessment of what is ‘necessary’ must be done in relation to the purposes for processing” (Torre, 2020). It may also differ from one individual to another, and it thus needs to consider this separately for each individual or for each group of individuals sharing relevant characteristics (see Information Commissioner’s Office, 2019).

Details of the blood groups of the employees from hazardous work are needed in case of an accident. Although adequate safety procedures for preventing accidents are taken, and such data may never be needed, there is much logic that it still needs to hold this information in case of emergency. However, holding by the employer such data of the rest of the workforce is likely to be irrelevant and excessive; that is to say, likely to be unlawful as they do not engage in the same hazardous work. Because the assessment of what data is needed should be based on the purposes of the processing itself, the data controller or processor should never have more data than what it needs to achieve the purposes of the processing (Information Commissioner’s Office, 2019). Then, it means collecting and holding only the minimum amount of personal data needed to fulfill the given purposes.

Another example goes on that ‘in case of gathering the data necessary to answer a particular research question, information that has no value for the research question, should not be collected. For instance, if you would like to build an email subscription list, only collect Name and Email. So, if you are collecting anything more than this (Date of Birth, Religion, etc.), then it might not be compliant with GDPR (Information Commissioner’s Office, 2019)’. Hence, any good data protection practice requires compliance with the principle. As what personal data should be collected and what should not, still remain in discussion, it is completely based on the specific-use-case.

Relevance is another crucial aspect when considering data minimization compliance. Accordingly, apart from a general questionnaire, the recruiters may ask for health conditions that are only relevant to particular manual occupations. An individual applying for an office job should not be asked for such information being irrelevant and excessive to the purpose. For instance, a local hospital to increase patient satisfaction with their care in the pediatric ward collects information at the time of patient check-in; and provides a choice candy to the patient on check out.

Collecting relevant personal information to the stated purpose of providing quality patient care would be considered, but sharing candy preference data with a third-party candy manufacturer would not appear so (see Tortoise & Hare, 2018).

The collection of personal data must not be on the off-chance, i.e., it might be useful in the future, but it may justifiably be so for a foreseeable event (Malek, 2020). Hence, in case of a breach of the data minimization principle, individuals will also have the right to erasure (Information Commissioner’s Office, 2019). Under the GDPR, if the personal data that deems incomplete or insufficient in achieving the purpose of the processing is not ‘adequate’; and considering the context and nature, individuals have the right to complete that data (the right to rectification) (see Torre, 2020). Even further processing

is, however, permissible if the new purpose is not incompatible with the old purpose. Individuals have also the right to get deleted any data that is not necessary for the purpose (the right to erasure, or the right to be forgotten). However, the GDPR also provides for an exception to the data minimization concept, which permits the longer retention of personal data for 'statistical purposes'.

In practice, the data minimization concept forces you to be more conscious about what data you collect. In case of violation of the mandate of the principle, legal actions can be taken by individuals in the European jurisdiction. According to Article 83(5)(a) of the GDPR, the infringements of the basic principles for processing personal data may lead to substantial administrative fines up to €20 million, or 4% of the total worldwide annual turnover. whichever is higher. In France, a fine of 250,000 Euro was imposed on an online retailer 'Spartoo' in August 2020 for a breach of the data minimization principle, among others, full and permanent recording of telephone calls received by customer service employees was held to be excessive. The recording and conservation by the online seller of customer bank details, communicated when orders are placed by telephone, was also 'not necessary' for the intended purpose (see GDPR Enforcement Tracker, 2018).

The data minimization approach is also included in the 2018 California Consumer Privacy Act (CCPA), and the 1988 (Australian) Privacy Act. In fact, "the first regulatory issue concerns personal data protection and consumer protection; then comes to ensuring the application of consumer law on Big Data technologies" (Malek, 2020). It is aptly put that "there are relatively few instances in which data protection authorities have forced technology firms to re-design their software, hardware, or business processes to minimize the processing of data or make it possible for data subjects to use such systems anonymously" (Rubinstein, 2013, p. 74). In conducting a data minimization evaluation, it is necessary to confirm that the collected data is adequate and relevant to the original purposes; and the burden of proving such compliance rests upon the organization.

4. Why Data Minimization Approach is Crucial.

As a risk-management measure, the data minimization approach has become an issue of great importance among information technology stakeholders. It is evident that between the European Union's General Data Protection Regulation (GDPR) and the growing liability of managing large volumes of data in one vulnerable database, businesses are taking a new look at the concept of data minimization (see business.com, 2020). Excess data has a vulnerability for businesses. Hence, it is expedient to point out that to minimize data is to reduce the risk.

Whereas costs are associated with every byte of data store, storing everything either in-house-data centers or cloud archiving is not only unviable but also unnecessary. As a result, traditional forms of data storage shift to lower physical occupancy of data. In fact, holding unnecessary data can bring you more harm than good. For example, as a phone with an overload of apps

and data begins to perform low, a company overflowing with unrequired data in storage begins to stagnate in the long run. Besides, in case of storing too much information, a data breach can be catastrophic when it happens. Even it may lead to charges of criminal negligence. It also costs money and time, and can become dangerous too.

Again, all data are not equally relevant and useful. In essence, much of that data will never be used. Although cloud storage as the latest option for storing data is not expensive, it does not encourage recording all the data and hoarding this excessive data indefinitely that we have. In the existence of such emerging problems, data minimization mitigates both these factors significantly for it stands as a solution to ensuring that we store the data relevant to our purpose. Since more data entails more threats, it is fair to opine that here comes up the relevancy of the notion-the bigger is not always better.

Lack of trust and anonymity has been considered for a long time as the main reason why some always put shopping offline first. By applying the concept of data minimization as a data protection principle, online dealers could reap the great potential benefits of increased online sales (see The International Association of Privacy Professionals, n.d.). The idea 'less data' to be provided may also result in to be much easier, quicker, and user-friendly in an online transaction (see The International Association of Privacy Professionals, n.d.). It should be a benefit for both the company and the individuals. Furthermore, Big Data becomes extremely valuable to the hackers[2] who intent to access to vast amount of data in order to commit fraud or identity theft, or introduce malware to control devices remotely. The risk of data loss and theft is also minimized when only the necessary data is stored up.

In Turkey, a bank faced sanctions for violating the principle of data minimization because the bank provided a six-month account statement of its customer to a civil court when the court only asked for the statement of the last three months (see Malek, 2020). As a result, for harnessing more benefits and mitigating risks, the pursuance of the principle palpably posits that collection or retention of fewer amounts of data is sometimes more in the Big Data world (see GDPR Enforcement Tracker, 2018).

In 2018, under the provision of the GDPR, The Danish Data Protection Authority fined a taxi company 'Taxa', an amount of 1.2 million kroner (US$180,000) for the preservation of the personal data relating to about 9 million individual taxi rides, beyond the lawful two-year retention policy. The regulatory body held that the authorities should also check out whether the data retention policy is duly made and carefully followed (see GDPR Enforcement Tracker, 2018). As it is argued that "companies are concerned about the loss or the leak of data that belongs to them and also about the loss of the personal data with which they have been entrusted" (Kirtley and Shally-Jensen, 2019, p.130), data minimization methods produces significant benefits that in fact include adhering to essential principles of data protection

2 See for example, Betsy Swan, Facial-Recognition Company That Works with Law Enforcement Says Entire Client List Was Stolen, The Daily Beast (February 26, 2020).<https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen>.

and EU GDPR compliance; decreasing internal and external threat surface areas; and reducing data storage costs (see Dataguise, n.d.).

Noticeably, privacy policies have thus expanded rapidly on commercial websites as fair practice, including the data minimization approach, to notify users about collecting and using their personal data, even in the absence of any comprehensive law that regulates the substance of privacy policies (see Malek, 2020). Although the data minimization approach is alleged to have crippling effects on Big Data analytics, it basically reduces cost and prevents data breaches from being catastrophic and subject to charges of criminal negligence.

5. Applying the Data Minimization Approach.

Although the practice of the data minimization approach is not an easy thing, it is not difficult too. While collecting personal data, the organizational responsibility comes with 'data classification' that help better to define the data; and decide which personal data is commensurate with the intended purposes or services. For example, in the case of medical service, gender may be more relevant than religion or ethnicity. Consequently, determining what data is absolutely necessary is the first step in a successful data minimization strategy (see business.com, 2020). In the context of European jurisdiction, it is provided that safeguards shall ensure the presence of technical and organizational measures in order to respect the principle of data minimization,[3] in a way that the requirements are not merely directed towards safeguards as such, but towards appropriate ones. Two kinds of safeguards are explicitly mentioned here, namely technical and organizational measures. In this context, practices on the concept of data minimization can be exemplified by pseudonymization and anonymization, i.e., when data is no longer personal data according to the GDPR (Article 2), and thus, falls outside the material scope (see Marcelo Corrales et al. ed., 2017).

The data minimization approach is also considered as DIY (do-it-yourself) data protection practices (see Matzner et al., 2016) that put the responsibility on individuals as the most immediate way to protect their personal data. The term DIY resonates with all measures taken by individual persons to protect their own data by way of, for example, the use of cryptography, pseudonymization and anonymization tools, browser plugins that manage cookies or block tracking and other tools used to minimize data collection.

In the DIY approach, there are passive and active data protection practices. Passive strategies include all strategies relying on withdrawal (opting-out) or data parsimony. Active strategies, on the other hand, encompass the use of privacy-enhancing technologies and taking legal actions. As such, "they serve to build a protected sphere, in which users can perform their selves without

[3]Article 89 (1), GDPR (2018); [Appropriate safeguards concern technical and organizational measures, respecting the data minimization, proportionality, and necessity principle. They may include the possibility of resorting to pseudonymization, where applicable, or further processing "which does not permit or no longer permits the identification of data subjects". The measures involved must take into account the impact on individuals, like physical or psychological potential damages they might suffer]. see GDPR-Text.com. [online] Available at: https://gdpr-text.com/read/article-89/ [Accessed 29 Jan. 2021].

worrying about potential privacy threats" (Matzner et al., 2016). Thus, in furtherance of these measures, the DIY approach requires fostering knowledge and awareness among the data subjects concerning data significance and security.

Moreover, the concept encourages periodically reviewing the data process in order to check whether the stored data is still relevant and adequate for the purposes. If irrelevant or excessive, then delete anything which is no longer needed. In fact, there is a pressing need to have clear and sound data policies on processing, retention, and access by design or by default, and delete and/or archive data on a periodic basis if the organization is holding duplicate and/or unused data. Service providers should have good reasons for asking for specific data. In the case of collecting data that is 'relevant' while creating a personal profile, for example, it is to fix first which data is important.

To exemplify as such, the company should also consider whether it could offer the same feature while collecting less information, such as by collecting zip code rather than precise geolocation. If the company does decide it needs the precise geolocation information, "it should provide a prominent disclosure about its collection and use of this information and obtain consumers' expressed consent. Finally, it should establish reasonable retention limits for the data it does collect" (National Cooperative Freight Research Program, 2019).

As aforesaid, the data minimization approach could boost up online sales in the online retailer's transactions. Hence, there should be no excuse to identify consumers in the name of warranties, potential claims, and taxes. It can be done in the same way as "when buying goods offline, unique product number and transaction details should fully suffice, unless specific laws and regulations require more data for a perfect reason" (The International Association of Privacy Professionals, n.d.). Hence, data classifications, and having clear and sound data policies on processing, retention, and access by design or by default, and reviewing data on a periodic basis can rescue ventures from data explosions.

Strategic data erasure is a core component of the data minimization methodology. User information has a lifespan, which has never been truer than in today's fast-moving digital marketplace. As a result, all data minimization plans should include deletion protocols (see business.com, 2020). User verification and screening through initial assessment procedures in place, organizations may gather only usable information from verified sources (see business.com, 2020).

Hence, there are some pragmatic approaches to minimizing data if the concerned authority respects the principle. On such premise, it is argued that "there are relatively few instances in which data protection authorities have forced technology firms to re-design their software, hardware, or business processes to minimize the processing of data or make it possible for data subjects to use such systems anonymously" (Rubinstein, 2013, p. 74). Considering the imports of the very concept as stated above with pertinent instances and expositions, it can be said that if one asks whether bigger is always better. The answer is in the negative. It is because "even in the realm

of Big Data, companies, and governments are beginning to see the value in a 'less is more' approach" (Marr, 2016).

6. Existing Dilemmas and the Way Out.

There is a dilemma whether data minimization can survive the onslaught of Big Data. In addressing the challenge, Article 23(2) of GDPR creates a more specific obligation for controllers to ensure 'by default' implement mechanisms that data minimization requirements are satisfied. Basically, it is not denying that merely existing of such specific obligation will not suffice because the efficacy of such measure much depends on how it is implemented. So, this new data protection requirement for 'by design and default' may be encouraging, but it still remains in the black box.

There is also another discourse that the "data minimization approach is inimical to the underlying thrust of Big Data, which discovers new correlations by applying sophisticated analytic techniques to massive data collection, and seeks to do so free of any ex-ante restrictions" (Rubinstein, 2013, p.78). It is also claimed that data minimization requirements have crippling effects on Big Data and its associated economic and social benefits. Hence, as it is arguably put that "the regulators should expect to oversee this requirement largely observed in the breach" (see Tene and Polonetsky, 2013). In fact, it is so likely that there should always be a check and balance in the governance mechanism. While companies and organizations are desperate to harness new promises of Big Data analytics, there should be a tool to minimize the associated risk and harm of misuse or abuse of the massive data collection and retention. It is the principle that can operate as such a check on data explosion and encroachment.

It is also argued that "Big Data challenges international privacy laws in several ways as it casts doubt on the distinction between personal and non-personal data, clashes with data minimization, and undermines informed choice" (Rubinstein, 2013). As Big Data is a more powerful version of knowledge discovery in databases or data mining, the dataset, whose size is beyond the ability of the typical database software to capture, store, manage, and analyze, or the nontrivial extractions of implicit, and previously unknown data, potentially poses complex challenges as well ((see Zarsky, 2003; McKinsey Global Institute, 2011).

As aforesaid, providing extra information is not always advantageous for the consumers too. So is also applicable to companies and organizations. In fact, this concept advocates for quality over quantity in a sense, for it imposes limits on the quantity of data that can be processed and requires digressive dada to be discarded.

Even less need may entail less risk of inaccuracy as well. However, discussing in volume the comparative advantages or disadvantages of data minimization and its legal implications requires an interdisciplinary study.

Basically, the GDPR comes as an established, recognized, and rescuing legal instrument which requires companies and organizations to minimize data collection to the extent of relevant, limited, and necessary threshold that can

instead encounter such potential risk of data tsunami. Provably, the data minimization concept is thus still of great relevance in the age of Big Data as it effectively embodies the notion revealing that less is more, sometimes. It is hereby aptly argued that “some information may not need to be collected or shared as initially planned, or the user can be given a choice over which data is processed, based on their functionality needs” (Marcelo Corrales et al. (ed.), 2017).

Conclusions.

The foregoing discourse makes it conspicuous that the preponderance of the data minimization concept largely depends on the consequences which may ensue upon data processing purposes and places. As a result, risk mitigation requires each byte of data processed and stored to be filtered through a series of objectives. If the data does not fit into any of the intended purposes, that should be discarded or deleted. Adopting mechanisms by design, and/or by default, or by cryptography offers the pragmatic way out in the jurisdictions where the concept is incorporated into their legal instruments as a legal principle.

Moreover, building awareness and sensitizing personal data in the Big Data context may also seemingly seem to be a pathway for the minimization initiatives at the social and business domains. At the individual level, the DIY approach is optimally encouraged for minimizing data collection with the tools like browser plugins that manage cookies or block tracking, or pseudonymization and anonymization tools, etc. Even in jurisdictions where regulation or the hard governing law is lacking, the proven benefits of minimizing unnecessary and digressive data collection and storage encourage companies and organizations to be prepared to pursue the approach as a general principle of data protection law. Every democratic society should embrace the same as a virtue as it legitimately limits the task from data collection to data transmission and retention.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

How legal design can improve data protection communication and make privacy policy more attractive.

CHIARA RAUCCIO
Lawyer in Rome and LL.M. at Tilburg University

Abstract

This article addresses the problem of communication of privacy policies, usually written by lawyers for lawyers using complex language and technical legal terms (so-called "legalese"). As such, data subjects barely read them or are not able to fully understand their meaning. In this scenario legal design may offer innovative solutions to draft and communicate more accessible and efficient privacy notices. In particular, legal design draws on the application of design mindsets and methodologies to the legal environment in order to make it more creative, communicative and user-centered.

Keywords: data protection; privacy notice; consent; transparency; GDPR; legal design.

Introduction.

On 4th January 2021 WhatsApp, the world-leading instant messaging app, notified its users an update of its terms of service (T&Cs) in relation to its privacy policy. The new T&Cs were meant to take effect from 8th February 2021 with the alert that users could not have continued to use the service without accepting the new terms.[1]

A few days later, on 15th January, WhatsApp announced to postpone the application of the new T&Cs for European users until 15th May 2021. The decision followed the intervention of the Italian Data Protection Authority ("Garante per la protezione dei dati personali" or simply "Garante") that contested the lack of clarity and intelligibility of the new privacy policy as far as it did not allow users to understand what changes had been introduced and, therefore, to make fully informed and free choices about the use of personal data.[2] The Italian DPA raised the issue before the European Data Protection Board (EDPB) so that a uniform position could have been taken by EU DPAs. As a result, WhatsApp decided to postpone the application of the new terms in order to have time to review the Garante's announcement and clarify the policy updates.[3]

What is most surprising about the WhatsApp case is that the Italian DPA did not criticise the content of the new privacy policy but rather the lack of clarity in its communication and the confusion it had caused among EU users, especially in relation to the sharing of data with the parent company Facebook. In particular, users got worried that under the new terms WhatsApp could have weakened the encryption of chat messages and would have shared them with Facebook. In reality, under the new terms personal messages between users remain end-to-end encrypted by default (meaning that only recipients can read them) and WhatsApp is not able to access users' chats nor share them with Facebook. The only personal data that WhatsApp can share are users' account information like phone number, access logs, device identifiers, IP addresses, and other details about the device. Yet, such data have been shared with Facebook since 2016 and nothing has changed under the new T&Cs. The update has only affected optional business features (when customers message a business through WhatsApp their data may be stored on Facebook's servers

[1] See WhatsApp's new Privacy Policy at https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en.
[2] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9519943#english_version.
[3] See WhatsApp's declaration on the WhatsApp Blog at https://blog.whatsapp.com/giving-more-time-for-our-recent-update.

and used for advertising).[4] There has been, thus, a clear communication failure.

The question is why a leading company as WhatsApp with billions of users and enough economic resources did not take care of developing a good privacy policy (not only in terms of content but also) in terms of form and did not invest in an effective communication campaign to announce it.

The most likely explanation is that the majority of companies today are not really interested in providing users with clear and transparent information about the services they offer and the way they process personal data. Their main interest is to look like formally compliant with the legal requirements imposed by the applicable legislation. Unfortunately, even today, three years after the GDPR come into force in May 2018,[5] data protection requirements are still considered just as formalistic swallow obligations, as boxes to tick in the "to-do list" to disclose to data protection authorities in the event of an audit. It follows that legal document like privacy notices, although addressed to data subjects, are often written in a language full of jargon and complex sentences (so-called "legalese") not really meant to be understood by the layman. The consequence is that data subjects generally ignore them entirely and, thus, are completely unaware of what really their personal data is used for, by whom and in what way, with the consequence that they cannot exercise an effective control over their data nor take meaningful and free decisions about it.

To deal with this practice, not only in the field of data protection but in the legal environment in general, a new discipline known as legal design is gaining attention. The concept of legal design was born around 2013 when a joint venture between Stanford's School of Design (commonly known as the D.School[6]) and the Law School was founded by Margaret Hagan[7] under the name of Legal Design Lab.[8] However, it is especially over the last few years that this discipline has started growing and developing in Europe thanks in particular to the work of Helena Haapio[9] and Stefania Passera.[10] Indeed, only

[4] See WhatsApp's clarifications about the new Privacy Policy at https://faq.whatsapp.com/general/security-and-privacy/answering-your-questions-about-whatsapps-privacy-policy.

[5] The Regulation (EU) 2016/679 was adopted on 14 April 2016 and became enforceable in all EU Member States on 25 May 2018.

[6] See at https://dschool.stanford.edu/.

[7] Margaret Hagan is a lawyer and a designer based at Stanford University. She is the Director of the Legal Design Lab, hosted at Stanford Law School's Center on the Legal Profession, and a lecturer at the Stanford D. School. Her work focuses on applying design to law in order to create more accessible and engaging legal services, and it is based on experimentation and a human-centered approach. See https://www.margarethagan.com/ .

[8] The Legal Design Lab is an interdisciplinary team based at Stanford Law School and D. School with the aim to build a new generation of legal products and services. It is based on human-centered design and empirical research to reimagine how the legal system could work. For more details see https://law.stanford.edu/organizations/pages/legal-design-lab/.

[9] Helena Haapio is a lawyer, contract innovator, and a pioneer of the proactive approach based in Helsinki. In her work she helps clients to use contracts and the law proactively to achieve better business results, balance risk with reward, and prevent problems. Her current multi-disciplinary research focuses on ways to transform contracts from legal instruments to valuable business tools. For more information see http://www.lexpert.com/our_team/more-about-helena_haapio/. Among her works see H Haapio, 'Next Generation Contracts: A Paradigm Shift' (2013) Doctoral dissertation, Lexpert Ltd.

[10] Stefania Passera is a designer, consultant, and researcher based in Espoo, Finland. She is specialized in contract design, simplification, and legal design, helping private and public organizations make their contracts, T&Cs, contract guides, policies, etc. user-friendly, visual, clear, and effective. She is also the creator of Legal Design Jams, the first workshop format aimed at innovating legal documents and prototyping hands-on. For more information see https://stefaniapassera.com/about/.

recently companies have begun to understand how important it is being clear and transparent with users in order to establish with them a relationship based on trust rather than on tricks.

As it will be explained more in-depth in the following sections, legal design can be generally defined as an interdisciplinary field of research and practice that tries to apply design-based methods, skills, and attitudes to the legal system in order to enhance legal communication and solve legal issues.[11] To that end several methods have been developed meant to pinpoint the main challenges of an area of law (e.g. data protection) and identify the best solutions to solve them.

In the present paper I will analyse the application of legal design to the field of data protection, in particular in relation to drafting and communicating privacy policies. The goal is to evaluate whether this approach may be effective in this area of practice and, if so, to what extent and how it can help legal practitioners to make privacy-related documents easily understandable and enjoyable to data subjects.

The paper is structured as follows. Section 1 will introduce the concept of legal design with a brief reference to its origin, its methodologies and the phases of the design process. Section 2 will then examine the state of the art in the process of designing and communicating privacy notices in order to identify the main problems currently existing in this field. In particular, the difficulties that data subjects usually face when approaching a privacy notice will be analysed to assess how they impact on the relationship between data controllers and users/data subjects and on the company reputation. Section 3 will dive into the application of legal design to the field of data protection and different tools will be examined that could help making privacy notices more attractive and understandable to data subjects and, thus, solve the problems posed by the traditional use of "legalese". Finally, the conclusions will suggest a reflection on the role of legal design in the development of more transparent privacy notices and its future in the field of data protection.

1. Legal design: an overview.

Legal design is a discipline that combines law, technology, and design to create user-friendly legal documents and, more in general, make the legal system closer and more accessible to people. The origin of legal design cannot be fixed on an exact date since broad discussions about applying some skills and methodologies of design to the field of law date back to the first decade of the new millennium.[12]

The concept of legal design draws on design thinking, a methodology to solve problems in a creative and human-centric way.[13] However, it was in the academic environment that these ideas were developed and brought forward.

[11] A Perry-Kessaris, 'Legal Design for Practice, Activism, Policy and Research' (2019) 46(2) Journal of Law and Society, 185-210.
[12] See, for instance, RL Martin, *Design of Business: Why Design Thinking is the Next Competitive Advantage* (Harvard Business Review Press, 2009); T Brown, *Change by Design: How Design Thinking Transforms Organizations and Inspires* (Harper Collins, 2009).
[13] On the history of design thinking see https://designthinking.ideo.com/history.

In particular, the first milestone is 2013, when Margaret Hagan founded at Stanford Law School and D. School the Legal Design Lab. Later on, the movement grew in Europe as well, in particular in Finland thanks to Helena Haapio, pioneer of proactive law,[14] and Stefania Passera, information designer expert in contract visualisation. Hagan, Haapio and Passera, together with other legal designers, created the Legal Design Alliance (LeDA), [15] an interdisciplinary network of academics and practitioners from both law and design that published on its website a manifesto of legal design.

Margaret Hagan in her e-book *Law by Design* defines legal design as "the application of human-centered design to the world of law, to make legal systems and services more human-centered, usable, and satisfying". [16] This definition makes it clear that the core of legal design is human-centeredness, meaning that any legal products should be designed and developed from a user perspective, i.e. thinking on what could be more engaging and accessible to the intended user. [17] Additional features of legal design, as outlined in the manifesto drafted by the LeDA, are proactivity and prevention, given that its purpose is driving desirable outcomes and preventing problems rather than dealing with the consequences of failure and trying to resolve conflicts already arisen.[18]

To achieve this result, the legal system should be rethought with an approach open to innovation and creativity and willing to collaborate with experts from different areas, in particular designers. In other words, designerly ways should be deployed to address lawyerly concerns [19] and lawyers themselves should develop creativity and communication skills. The starting point should be no longer what a legal document shall include to comply with the law, but rather how it can be organised and displayed in such a way to be understandable and usable by its recipients.[20]

Legal design may be referred to any area of law like legal research, access to justice and governmental policy.[21] However, so far it has been mostly deployed for legal documents like contracts, terms of service and privacy policies that, being addressed to common citizens (i.e. non-lawyers) pose major problems in terms of visualisation and communication.

In her book Hagan identifies three goals of legal design: (i) Helping the lay person and the legal professional; (ii) Creating a better front-end to the legal system and a better back-end; and (iii) Working for incremental short-term

[14] Proactive law is a legal approach that focuses on achieving positive goals and outcomes: it tries to prevent problems and disputes from arising rather than to resolve conflicts afterwards. To that end it stresses the importance of the needs and relationships of all those who use the law, not only legal experts but also laypeople.
[15] See Legal Design Alliance website, at <https://www.legaldesignalliance.org>.
[16] M Hagan, *Law by Design* (2017) at https://lawbydesign.co/.
[17] https://medium.com/astec/legal-design-and-the-challenges-of-innovation-in-law-cb9608132940.
[18] R Ducato *et al.*, 'Legal Design Manifesto' v1, available at https://docs.google.com/document/d/1FOLI4jHy6-rpEop9aOeY7BFZFPq_rRL8vzCB92s1a6c/edit?usp=sharing.
[19] A Perry-Kessaris, 'Legal Design for Practice, Activism, Policy and Research' (n 10).
[20] D Sless, 'Designing Documents for People to Use' (2018) 4(2) The Journal of Design, Economics, and Innovation, 125-142.
[21] For instance, for legal design in legislative drafting see L Aulino, 'Legal Design and Artificial Intelligence in support of legislative drafting during crisis' (2020) EJPLT.

improvements and breakthrough long-term change.[22]

As mentioned before, legal design relies on design thinking, a process that uses design to solve problems (of any kind, not just legal) from a human-centric perspective. As such, legal design is based on designerly mindsets and methodologies, with the consequence that lawyers have to set aside the traditional legal approach (quite conservative and focused on the essence of the rules more than on the accessibility to the intended recipients) and embrace a designer's mindset. This does not mean that lawyers need to become designers themselves, but they should combine skills, knowledge, and attitudes that are both designerly and lawyerly. In particular, lawyers should learn from designers the importance of communication and experimentation as means to pinpoint the issues faced by users, identify their expectations and find solutions to meet them.

Legal design has borrowed from design thinking not only its mindset, but its methodology as well, thus paying particular attention on exploration and experimentation.[23] Although several methodologies exist and different sets of methodologies may be combined in different ways, it is possible to define the basic flow of the legal design process[24] and the following stages can be identified.[25]

- Stage 1: Discovery and Understanding. This phase is meant to understand the main challenges of the area of interest, namely the major problems that users usually face when dealing with a certain task (e.g. reading the terms and conditions of a service, or a privacy notice). The most effective way to achieve this aim is getting in contact with the parties involved in order to understand their perspective through interviews, observations, data gathering, and exploratory workshops.
- Stage 2: Synthesize. After all the information has been gathered, the second step requires to select only the most relevant ones in order to identify only the main challenges upon which the rest of the design process will be focused (indeed, too broad topics cannot be effectively dealt with). To that end, it is necessary to limit the target users and prioritise the issues that have been raised.
- Stage 3: Brainstorm and Build. The third stage is generative and constructive since it aims at coming up with new ideas and prototyping them out. In this stage brainstorming and creativity are crucial: all the members of the team have to start thinking together about possible solutions to the challenges previously identified. Brainstorming should be

[22] M Hagan, *Law by Design* (n 38).

[23] Different methodologies exist in the field of design thinking, yet they are mostly based on common elements. For example, the Design Council has identified four phases of the design process: Discover, Define, Develop, and Deliver. On the other hand, the D. School at Stanford offers a hexagon-based vision of design thinking composed of five phases: Empathize, Define, Ideate, Prototype, Test (see D. School, 'A Virtual Crash Course in Design Thinking', at https://dschool.stanford.edu/resources-collections/a-virtual-crash-course-in-design-thinking).

[24] The stages as described in this section have been identified and developed by M Hagan, *Law by Design* (n 38).

[25] A more detailed description of the process can be found in T Brown, *Design Thinking* (Harvard Business Review, 2008); L Kimbell and J Julier, *The Social Design Methods Menu* (Fieldstudio, 2012), 1–56; L Carlgren *et al.*, 'Framing Design Thinking: The Concept in Idea and Enactment' (2016) 25(1) Creativity and Innovation Management», vol. 25, 38–57.

based not only on the invention of something completely new, but also on the research and analysis of existing patterns, models, and templates that may become remarkable sources of inspiration. Once enough ideas have been put forward, the team has to choose the one(s) to pursue.[26] Only the ideas that have been chosen will be prototyped. Prototypes are tested for usability, experience, and feasibility and through continuous testing and brainstorming they are gradually improved to get closer to the solution of the challenges concerned.

- Stage 4: Test, Iterate and Scale. In this stage the ideas that have been selected and prototyped must be tested to refine them and get closer to the final version. Testing means implementing the ideas into the real word towards the targeted users and analyse how they react and welcome them. The users' feedback becomes essential to understand whether the intended recipients will approve the prototyped idea, will be willing to use it and will find it useful and in accordance with their needs. This is the only way to know whether the ideas that have been brainstormed are promising and able to solve the identified problems and, thus, avoid wasting time and resources on unsuccessful paths.
- Stage 5: Scaling, Evolving and Implementing. If the feedback has been positive, it is possible to start thinking on how to turn the prototype into a real thing. To that end it is important to develop a plan of implementation that defines the main features that the final outcome should have and the timing to implement them. Such a plan would require the engagement of all the team members but also of external partners.

As seen, the core of the design process described above is experimentation. Designers cannot think to come up with the final version in the first stage of the process but, on the contrary, the starting point is a brainstorming where multiple and different ideas are proposed. Only a few of them will be considered good enough to meet the users' expectation and, thus, will be further developed and prototyped. Even less will be actually put in practice and tested and, anyway, they will be continuously refined and improved, also on the basis of users' feedback, to reach the final and definite version. Only this process of continuous testing and modifying can lead, in the end, to build the optimum solution. On the contrary, lawyers tend to put great effort in the first phase to find immediately the best solution and then implement it without prototyping and testing it. On this regard, Hagan observes that if lawyers <<think of everything [they] do as a prototype rather than as something that must be perfect, [they] can act more creatively and tap into others' creativity and expertise … It will also save [them] from falling too in love with ideas before they have figured out if they're workable>>.[27]

Some criticisms have been moved to legal design based on the fact that law is traditionally a verbal language, meaning that it expresses concepts by means of words. As a consequence, some scholars argue that the use of visual elements (e.g. icons, images, graphics) would enhance rather than reduce the

[26] Different strategies can be used to make this choice. For example, Margaret Hagan proposes the difficulty/importance matrix as a tool to evaluate which ideas are the best ones to pursue according to their feasibility, priority, and viability.
[27] M Hagan, *Law by Design* (n 38).

risk of misinterpretation and misunderstanding of legal documents given that they are not as precise as words to express legal concepts.[28] In addition, visual elements do not have a unique and certain meaning and different interpretations could arise depending on the context and the background of the recipients (e.g. geographical area, cultural background).[29] On the other hand, the supporters of legal design clarify that while in some cases visual elements may be even more precise and immediate than writing (e.g. traffic signs), in other cases they are not meant to replace words but rather to accompany them in order to clarify their meaning and help navigate the text.[30] As for the problem of interpretation, the same applies to legal words whose interpretation is not certain, on the contrary it is often disputed. In any case, it is not excluded that a common interpretation of visual elements can be developed and learnt over time.

Another criticisms to legal design is the risk of differentiation and potential discrimination between the recipients who read the written document – and understand technical legal terms – and those who rely on the visual elements. The latter could be penalised because the information delivered through visual design is more synthetic than the concepts expressed with words. Even this argument seems flawed firstly because visual elements may help lay people to better understand the meaning of legal words – thus becoming a support to the text – and secondly because people who do not have the expertise to understand legal writing – and, as such, would have no information at all – may at least rely on visual elements to grasp the meaning of the text.

2. The problem of clarity of law and the main communication challenges for data protection.

Legal design as described in the previous section may represent a paramount instrument to re-think the role and the function of privacy notice not only in relation to the structure and content of the document, but also its visualisation and presentation in order to provide data subjects with clear information and allow them to maintain effective control over their personal data. More in general legal design may help legal practitioners to face the issues of clarity and understandability of the law. This theme has old roots and has long been discussed among legal and linguistic scholars, especially in the United States.

The first modern massive study on the failure of law language was carried out by David Mellinkof, lawyer and professor of law at UCLA School of Law who wrote several books and articles attacking the excessive verbosity and impenetrability of legal writing. His first and most famous work is the 1963

[28] See for example S Esayas et al., *Is a Picture Worth a Thousand Terms? Visualising Contract Terms and Data Protection Requirements for Cloud Computing Users* in International Conference on Web Engineering (Cham, Switzerland, Springer, 2016) and JA Mitchell, 'Whiteboard and Black-Letter: Visual Communication in Commercial Contracts' (2018) 20 University of Pennsylvania Journal of Business Law, 837–43.

[29] See for instance S Isherwood et al., "Icon Identification in Context: The Changing Role of Icon Characteristics with User Experience," Human Factors 49, no. 3 (2007): 465 and R Dewar, "Design and Evaluation of Public Information Symbols," in Visual Information for Everyday Use: Design and Research Perspectives, ed. Harms Zwaga et al. (London: Taylor & Francis, 1999), 285–303.

[30] H Haapio and S Passera, *Contracts as Interfaces: Exploring Visual Representation Patterns in Contract Design*, in Legal Informatics, ed. Daniel Katz et al. (Cambridge: Cambridge University Press, 2016).

book "*The Language of the Law*" that analyses the history of English legal words and the evolution of a language that is technical, formalistic and obscure to lay people and lawyers themselves, thus causing misunderstandings and disputes.[31] On the same note is "*Plain English for Lawyers*" by Richard C. Wydick, an article published in 1978 that critics the incapacity of lawyers to write in plain English and the use of arcane and redundant phrases to express common concepts thus making the legal writing style "(1) wordy, (2) unclear, (3) pompous, and (4) dull".[32] These themes were further developed in the next years by the so-called "plain English movement" born in 1975 in the United States with the aim to make legal documents understandable by consumers who sign them.[33] Within this movement the concept of "information overload" was firstly elaborated referring to the accumulation of disclosed information that make it less available to consumers and thus useless.[34] According to the movement providing consumers with information is not sufficient: such information should also be understood by its intended recipients to be effective. The emphasis, thus, is shifted from information to communication.[35]

Since the abovementioned studies the issue of understandability of law and clarity of information has recurred in legal debates both in the Unites States and in Europe widening from contracts to any other area of law, including data protection. This explains the central role that the principle of transparency and the information duties play within the EU data protection legislation.

Indeed, the EU General Data Protection Regulation (GDPR)[36] adopted in 2016 and applicable in all the EU Member States since 25th May 2018 has introduced, among other things, a series of fundamental principles that any processing of personal data should be based on. One of those is the principle of transparency set forth by Art. 5 (1)(a)[37] that imposes on the data controller an obligation to keep data subjects informed about how their data is being used. The principle is further clarified in Recital 39 according to which transparency implies that data subjects are made aware that personal data concerning them are collected, used, consulted or otherwise processed, and such information should be easily accessible, easy to understand, and provided in a clear and plain language.[38] In addition, natural persons should be informed of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.[39]

The principle of transparency is further elaborated in several other provisions of the Regulation. First of all, Art. 12 states that any information and

[31] D Mellinkoff, *The Language of the Law* (Little, Brown and Co. 1963).
[32] RC Wydick, 'Plain English for lawyers' (1978) 66(4) California Law Review, 727-766.
[33] The beginning of the plain English movement dates to January 1, 1975, when the Citibank of New York introduced a plain English consumer promissory note leading New York to became in 1977 the first US state to pass legislation requiring plain English in consumer contracts and leases. See C Felsenfeld, 'The Plain English Movement in the United States' (1981-1982) 6 Can. Bus. L.J. 408.
[34] C Felsenfeld and AM Siegel, *Writing Contracts in Plain English* (St. Paul, West Publishing Co. 1981).
[35] *Ibid.*
[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
[37] Art. 5 (1)(a) GDPR states that "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".
[38] Recital 39 GDPR.
[39] *Ibid.*

any communication that the controller shall refer to the data subjects under the Regulation must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for information addressed specifically to children. The provision adds that the information may be provided in writing or in any other means, including, where appropriate, by electronic means and, when requested by the data subject, may be provided orally, provided that the identity of the data subject is proven by other means.[40]

Secondly, Arts. 13 and 14 GDPR list the information that data controllers and processors should provide data subjects with when personal data is collected, respectively, directly from the data subject (Art. 13) or from third parties (art. 14) in order to inform them about the processing. The required information includes, in particular, the identity of the data controller, the kind of data processed, the purposes of processing, the legal basis to process data, the period of storage of data, the existence of automated decision-making, including profiling.[41]

Furthermore, the principle of transparency applies in relation to consent, when it is used as the legal basis for processing. Indeed, a valid consent must be informed, meaning that the data subject must receive all the information about the processing to meaningfully decide whether or not to give his/her consent.[42] Transparency also concerns the way in which consent is required: when consent is given in the context of a written declaration that also concerns other matters, the request for consent should be clearly distinguishable and presented in an intelligible and easily accessible form, using clear and plain language.[43]

The principle of transparency has also been analysed by the Art. 29 Working Party (WP29) in its "Guidelines on transparency under Regulation 2016/679" adopted on 29 November 2017.[44] The WP29 explains that the concept of transparency under the GDPR is strictly linked to the principles of fairness and accountability – both set forth by Art. 5(1)(a) as well – and may refer to three central areas: (i) the provision of information to data subjects related to fair processing; (ii) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (iii) how data controllers facilitate the exercise by data subjects of their rights.

The rationale behind the principle of transparency, as confirmed by the WP29 itself, is to reduce the information asymmetry naturally existing between data controllers and data subjects when personal data is processed.[45] To that end data subjects should be made fully aware of the processing of personal data related to them and, thus, be empowered to exercise control over their data and exercise the rights granted to them by the GDPR.[46]

---

[40] Art. 12 (1) GDPR.
[41] Arts. 13 and 14 GDPR.
[42] Recital 32 GDPR.
[43] Art. 7 (2) GDPR.
[44] WP29, "Guidelines on Transparency under Regulation 2016/679", 11 April 2018, WP260 rev.01.
[45] A Rossi, R Ducato, H Haapio, S Passera, 'When Design Met Law: Design Patterns for Information Transparency' (2019) 1 Droit de la consommation – Consumentenrecht (DCCR), 79–122.
[46] The same technique is used in the field of consumer protection law. See, for instance, GK Hadfield, R Howse, MJ Trebilcock, 'Information-Based Principles for Rethinking Consumer Protection Policy' (1998)

However, in spite of the EU legislator's attempt to regulate the matter, this goal has been poorly achieved causing what has been considered a regulatory failure.[47] Indeed, although almost all data controllers have drafted or updated their privacy notice in accordance with the Regulation requirements and they usually provide data subjects with it, it could be hardly said that data subjects are actually aware of the processing of personal data related to them. The reason is that they usually do not read privacy notices but simply skip them, give their consent whenever it is required (even when it would not be necessary) and accept any terms of service. As such, it is not surprising that the sentence "I agree to these terms and conditions" has been called the "biggest lie on the internet".[48] The reason is twofold.

On the one hand, users are overwhelmed by T&Cs and privacy notices since anytime they access a website or ask for a service receive a notice explaining the terms of the service, the privacy policy and, for websites, the cookie policy. The result is that there are so many notices that it would be incredibly time-consuming reading all of them and no one has the time nor the willingness to do it.[49] On the other hand, privacy notices, just as any legal documents, are traditionally written in a language though by lawyers for lawyers and extremely difficult to understand for laymen, the so-called "legalese" which uses jargons, uncommon words, technical terms and long sentences. It follows that reading a privacy policy requires a lot of time, strong attention, and technical knowledge, with the result that users are discouraged from reading it and, even when decide to do it, do not really understand the meaning of what they read.

This practice is likely based both on the traditional idea that lawyers shall use their own language not accessible to non-lawyers as a symbol of their professional role, and on the traditional view that legal documents must be accurate, precise, and specific and only legal terms can effectively reach such a result, having an exact meaning that can describe a given concept without requiring other words. In this perspective, lawyers spend much time and effort to write long and comprehensive privacy policies in order to accurately describe the data processing and all the existing rights and obligations as required by the GDPR. However, in such a way the pursued aim may only be achieved when the documents are addressed to expert recipients who understand the legal terms and know how to interpret them (actually, even in this case, problems of interpretation can arise). On the contrary, this approach becomes completely flawed when the document is addressed to people who are mostly not lawyers and, as such, cannot understand the terms and the jargon used in the text.

This approach fails because it only focuses on the black letter of the law while does not take into account the needs and abilities of the individuals who the law aims to protect. In other words, this approach pays more attention to

21(2) Journal of Consumer Policy», 131-169. See also A Oehler, S Wendt, 'Good Consumer Information: The Information Paradigm at Its (Dead) End?' (2017) 40(2) Journal of Consumer Policy», 179-191.

[47] On the same topic, although in a different context, see O Ben-Shahar, CE Schneider, 'The failure of mandated disclosure' (2011) 159(3) University of Pennsylvania Law Review, 647-749.

[48] JA Obar, A Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2016) TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy», 1-37.

[49] In 2008 two researchers published a paper suggesting that reading all of the privacy policies an average Internet user encounters in a year would take 76 workdays. For more details, see AM Mcdonald, LF Cranor, 'The Cost of Reading Privacy Policies' (2008) Journal of Law and Policy for the Information Society.

formalistic requirements than to the substance of the rules, with the consequence, in fact, to water down the rules themselves.[50] Indeed, rules are meaningful as long as they are instrumental in achieving their goals and, in the field of data protection, the goal is to protect data subjects and allow them to exercise full control over their personal data. Therefore, it is crucial that privacy notices are clear and easily accessible: they may be regarded as instructions meant to explain data subjects how their personal data is going to be processed, what rights they can exercise in relation to the processing and how they can exercise them.

In this perspective the WP29 outlined in its Guidelines that the principle of transparency and the information duties in the GDPR are "*user-centric rather than legalistic*" meaning that "*the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects*".[51] To that end the Regulation includes specific and practical information requirements imposed on data controllers and processors. For instance, Art. 12 requires using a concise, transparent, intelligible and easily accessible form as well as clear and plain language and gives directives on the means to provide the information. In addition, it acknowledges the importance of visualisation and promotes the use of icons to enhance transparency.[52]

Such practical requirements are a way to guide data controllers and processors in providing data subjects with all the relevant information about the processing and ensure that such information is delivered in an efficient and effective way, so that the rationale behind the information duties (i.e., empowering data subjects to exercise control over their personal data) may be achieved.

Unfortunately, most data controllers and processors still consider these practical information requirements as formalistic obligations that they must strictly apply to be compliant with the law. The consequence, as seen in the WhatsApp case, is that controllers make a great effort to design complete and comprehensive privacy notices that include all the information listed in Arts. 13 and 14 GDPR and are formally and juridically correct. Yet, they do not consider at all the visualisation of the privacy policy, namely its structure, the way it is presented to data subjects and whether it is enough clear and accessible to them.

The result is a substantial violation of the GDPR provisions. Indeed, the human-centric perspective adopted by the EU legislator and outlined by the WP29 shifts the attention from legal compliance (i.e., an external application of the rules) to individuals' protection and, from this point of view, the information duties imposed by the GDPR are really complied only when the required information reaches the intended recipients. This means that if the privacy notice includes all the elements prescribed by Arts. 13 and 14 GDPR but

[50] S Passera, 'Beyond the wall of text: How information design can make contracts user-friendly', in A Marcus (ed.), *Design, User Experience, and Usability: Users and Interactions*, (Lecture Notes in Computer Science, Cham, Springer, 2015), 341-52.
[51] WP29, "Guidelines on Transparency under Regulation 2016/679", 11 April 2018, WP260 rev.01.
[52] Art. 12(7) GDPR states that "The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing". See also Recital 60.

does not catch data subjects' attention so that they don't read it or, even after reading, they cannot understand the meaning of the text, then the data controller should be considered substantially breaching the information obligation imposed by Art. 12 GDPR. Shouldn't that be the case, the principle of transparency would become a void concept in contrast with the principle of accountability that holds data controllers accountable for the measures adopted to ensure an adequate level of protection of personal data.

This is what happened to WhatsApp that, despite developing a correct privacy notice, has not been able to clearly communicate the update to its users who have thus misinterpreted the new terms and have got worried for a processing that, in reality, does not concern their personal messages, but only optional business features. There is no doubt that in this case the aim of the information duties has not been achieved due to a communication failure.

Communication failures in the field of data protection are, unfortunately, quite common and may be related to several issues. Haapio et el. have identified the most recurring hurdles to effective legal communication.[53] I will list below some of the most relevant hurdles classified according to their relation to (i) language, (ii) structure and visualisation, and (iii) presentation and communication of the privacy notice.

(i) When language is concerned, the main mistake commonly made by data controllers is the use of a highly technical and complex language difficult to understand without legal advice,[54] and the use of vague terms open to multiple interpretation (e.g. «might», «may», «reasonable effort»).[55]

(ii) As for the visualisation of privacy notices, the main problem is the well-known "wall of text",[56] a practice whereby the notice is structured as a column of words written with small font size without any spaces between the lines, any (or minimal) paragraphs and headlines, any images representing and exemplifying the meaning of the text. In addition, the text is often small-printed and excessively long, causing an information overload. The consequence is that data subjects are discouraged from reading it – since the text is perceived as impenetrable[57] – or, if reading, cannot keep the attention on the whole text because are not guided in the navigation and, as such, are not able to find the most important information in the text.

(iii) When it comes to the presentation and communication of the privacy notice, the main issue is the widespread use of standard (sometimes

[53] H Haapio *et al.*, 'Legal Design Patterns for Privacy' in E Schweighofer, F Kummer, W Hotzendorfer and G Borges (eds.), *Data Protection/LegalTech. Proceedings of the 21st International Legal Informatics Symposium IRIS 2018* (Editions Weblaw, 2018), 445–450.

[54] B Fabian, T Ermakova, T Lentz, 'Large-scale readability analysis of privacy policies', (2017) Proceedings of the International Conference on Web Intelligence (WI '17). Association for Computing Machinery, 18–25. See also C Jensen, C Potts, 'Privacy policies as decision-making tools: an evaluation of online privacy notices' (2004) Proceedings of the SIGCHI conference on Human Factors in Computing Systems, 471-8; JA Obar, A Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (n 23); N Robinson *et al.*, 'Review of the European Data Protection Directive' (sponsored by the ICO) (2009) RAND Europe.

[55] I Polloch, 'A typology of communicative strategies in online privacy policies: Ethics, power and informed consent', (2005) 62(3) Journal of Business Ethics, 221-235. See also JR Reidenberg *et al.*, 'Ambiguity in privacy policies and the impact of regulation' (2016) 45(2) The Journal of Legal Studies, 163-90.

[56] S Passera, 'Beyond the wall of text: How information design can make contracts user-friendly' (n 25).

[57] European Data Protection Supervisor, Opinion 4/2015 Towards a New Digital Ethics, 2015.

even pre-filled) documents that do not differentiate the targets and, as such, do not take into account the specific information needs and cognitive capabilities of the notice's addressees. Indeed, especially when a service is offered to different categories of users (e.g. children, elderly people, people with different socio-economic status and educational background), as it is the case, for instance, with social networks, the same language – in particular when it is complex and technical as seen in the previous point (i) – may not be adequate to all of them since they have different approaches towards the notice and different exigencies that cannot be ignored.[58] A further problem is the wrong timing of presentation of the privacy notices, given that they are usually presented when users are accessing to the service (e.g. they are entering on the website or concluding the purchasing process). In such a way the privacy notice is perceived by users as an obstacle that stands between them and the achievement of their purpose. Therefore, it is quite obvious that data subjects will ignore the notice and accept anything as long as they can quickly carry out their task and avoid any further disturbances.[59]

3. Legal design applied to privacy policies.

In accordance with the methodologies presented in Section 1, over the years legal designers have developed different solutions that can help solving the most recurring problems that people face when dealing with legal documents. Such solutions can be customised and re-used in different areas of interest according to the given problems. For this reason, they are known as "design patterns", a sort of best practices and standards shared among practitioners to provide the best solution to a recurring problem.[60] Their function is helping practitioners to make the legal document efficient and user-centered and, in such a way, to build general legal principles and create a common and unitarian legal practice. Over the last few years, several legal design patterns have emerged and many of them have been collected in open pattern libraries (freely accessible to anyone).[61]

In particular, several legal design patterns have been developed in the field of data protection or, even though developed in other fields, may be applied to it, especially to privacy notices, in order to solve the most recurring problems as listed in Section 2. The aim is to make the notice more user-friendly, namely

[58] H Haapio *et al.*, 'Legal Design Patterns for Privacy' (n 28).
[59] B Friedman, P Lin, JK Miller, 'Informed consent by design' (2001) Security and Usability, 503-530.
[60] The idea of patterns has originally been conceived in architecture by Christopher Alexander et al. (C Alexander *et al.*, *A Pattern Language – Towns, Buildings, Construction* (Oxford University Press, 1977). Then, design patterns have extended to many other fields, such as computer science, interface design, information systems, and biology.
[61] For an overview of legal design patterns, see for example H Haapio *et al.*, 'Legal Design Patterns for Privacy' (n 28); A Rossi *et al.*, 'Legal Design Patterns: Towards A New Language for Legal Information Design', in E Schweighofer, F Kummer and A Saarenpää (eds.), *Internet of Things. Proceedings of the 22nd International Legal Informatics Symposium IRIS 2019* (Editions Weblaw, 2019), 517-26; H Haapio, S Passera, 'Contracts as Interfaces: Exploring Visual Representation Patterns in Contract Design, in DM Katz, M Bommarito and R Dolin (eds.), *Legal Informatics* (Cambridge University Press, in press), 213-238.

easier for data subjects to understand. As a result, data subjects would be more willing to read the information and take meaningful decisions about data processing rather than just skip it and unconsciously provide (or refuse) any consents.

Design patterns as well may be classified depending on whether they relate to (a) the language used in the privacy notice, (b) the structure of the document, (c) the way the notice is presented and communicated to data subjects and, more generally, the user experience. I will analyse below some of the most interesting design patterns for each category.

a) The first element to consider is the language. Given that the notice is addressed to data subjects and is meant to explain them under which terms their personal data is going to be processed, the language should be tailored on the knowledge and the cognitive capacities of the intended recipients. Therefore, given that data subjects are (in most cases) common people (i.e. non-lawyers) and don't know legal technical terms (i.e. "legalese"), the language should be plain and intelligible, with short sentences and commonly used words. Special attention should be paid when the notice is addressed also or only to young people and/or children. In that case the language should be used accordingly, with children-friendly words and grammatical structures.
b) Structure as well has a huge impact on the comprehension of the notice. In order to avoid the wall of text seen in Section 2, the document has to be organised in a handful and intuitive manner, in such a way that data subjects can easily navigate the text and find the topics they are looking for. In particular, the sections (e.g. data controller's details, categories of data, purposes of the processing) should be clearly identified with meaningful headlines and spaces between the paragraphs. In addition, at the beginning of the document (or on one side) it may be helpful to include a table of contents with hyperlinks to the paragraphs that allow the readers to have an overview of the notice and go directly to the paragraph of interest. Another remarkable way to make the privacy notice more effective in terms of structure is building a layered notice.[62] This means that the relevant information is not provided at once, but it is layered based on the data subjects' cognitive capabilities, available time and willingness to read it and further information is displayed at users' request (for example, by pressing the button "Read more"). At first only the most important information is provided (e.g. the purposes of processing, the identity of the controller, the description of data subjects' rights), in a very synthetic and easily understandable form, in such a way that data subjects can rapidly grab the main points and have an overview of the data processing. Then, if they are interested in knowing the processing more in-depth, additional information will be provided (even using more technical terms addressed to expert readers like lawyers and supervisory authorities).[63]

[62] The importance of layered notices has also been outlined by the WP29 in its guidelines on transparency. See WP29, 'Guidelines on Transparency under Regulation 2016/679', 11 April 2018, WP260 rev.01.
[63] A good example in the European panorama is offered by the UK startup Juro that developed its privacy policy based on a layered approach. When opening Juro's website, the short version of the privacy policy (called "Your privacy at a glance") pops up as a modal window displayed on just one screen of a typical

In any case the first layer, although more accessible and synthetic, needs to include all the information necessary to make data subjects understand the data processing in its entirety, including its risks. Thus, it cannot include only fair terms, whereas unfair or risky practices are hidden in the other layers.[64]

c) When drafting a privacy notice, the way it is presented and communicated to the intended recipients cannot be overlooked. Assuming that the information is written in plain language and the text is coherently structured, if its presentation is not enough "catchy" data subjects will hardly read it. As explained by the cognitive load theory,[65] when reading a text the human brain tends to avoid an information overload and, to that end, tries to find strategies that minimise the information process and make the text comprehension easier, for example by associating new information to pre-existing models, or by skimming the text to find just the information needed. Good designers are able to structure the document in such a way to reduce the brain workload and eventually make it less stressful and exhausting to read the text. For this reason it is important to include visual elements that may immediately catch the reader's attention and that the brain can easily associate to broader concepts.

Several design patterns exist to improve document visualisation. The first solution is the provision of illustrative examples that apply the abstract and vague legal concepts to a factual situation which the readers can more easily relate to and, thus, understand. Another useful tool is the FAQs section, where the most common and foreseeable questions are listed, and a brief and synthetic answer is provided for each of them. This system allows data subjects to immediately find the information they are likely looking for without having to read the whole document, but also to understand what the most relevant topics in the notice are.

One of the most interesting and innovative tools are icons, namely graphical elements usually added at the beginning of a paragraph that, through simple images, can attract attention, give an idea of the content of that paragraph and help finding and memorising the information they relate to. Icons usually are not used alone but more commonly accompany the text, given that they are not self-explanatory; nevertheless, they are incredibly useful to help users navigate the text and have at a glance an overview of the information provided in the document and the paragraph where it is displayed. Indeed, images are easily and immediately processed by the human brain without causing a work overload and, in addition, they usually catch the reader's attention by interrupting the wall of text. Thus, it is more likely that data subjects will look at them (and reading the accompanied text).

The use of icons in the privacy notice is allowed by the European legislator itself; in fact, Art. 12 (7) GDPR, in relation to the provision of transparent

---

browser. It only includes the key facts and users have the chance to click through to the full policy if they want to read more. See Juro's website at https://juro.com/policy.html.

[64] On this point see the Norwegian Consumer Council in the case of the presentation of Facebook's facial recognition feature, see Norwegian Consumer Council, 'Deceived by Design', (2018), at https://fil.forbruker-radet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[65] The cognitive load theory (CLT) was originally developed by Sweller while studying problem solving. See J Sweller, 'Cognitive Load During Problem Solving: Effects on Learning' (1988) 12(2) Cognitive Sci., 257–285.

information and modalities for the exercise of data subjects' rights, states that "*The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing*".[66] On the same line, national Data Protection Authorities (DPAs) are encouraging data controllers to deploy icons in their notices in order to make them more intelligible and enhance data subjects' control over personal data. In particular, it is worth a mention the recent initiative of the Italian Garante that in March 2021 launched a contest calling for creative solutions to make information notices simpler, clearer and immediately understandable through icons, symbols or other graphic elements. The three datasets of symbols and icons that will be considered especially effective will be selected and made available on the Garante's website for use by all stakeholders, specifying the author's name.[67] Such an initiative confirms that attention is being paid even by institutions on the fact that the information notices used so far by most companies, websites, social networks, and other controllers are often too lengthy and complex and, thus, unable to fulfil their essential function (i.e., informing data subjects about how their personal data are used and allowing them to maintain control over such data). Moreover, the fact that a DPA has launched a contest for the creation of icons means that legal design has been acknowledged as an effective instrument to make privacy notices more accessible and, thus, closer to their function.

As far as document visualisation is concerned, additional solutions exist to make privacy notices more attractive, especially when they are addressed to young people. In certain cases the content of the notice may be represented as a cartoon that, with a combination of images and text, makes the legal concepts much easier and even fun. The risk of this solution is an oversimplification of concepts, given that it is difficult to cover all the topics relevant to the data processing by means of cartoons.[68] Therefore, it may be useful to explain basic concepts to children but cannot replace a textual notice for adult data subjects.

Finally, a peculiar way to provide data subjects with the information notice is through gamification, meaning that the information related to the data processing is displayed in a gamified environment.[69] Game-based learning is a technique – already used in other fields like cybersecurity – that integrates games into instructional content by incorporating the characteristics of computer games to engage users.[70] Data subjects can interact in a virtual

[66] Art. 12 (7) GDPR.

[67] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9561395#english_version.

[68] RG Anaraky *et al.*, 'Testing a comic-based privacy policy' (2019) The 15th Symposium on Usable Privacy and Security.

[69] One of the first experiments in this field was "PrivacyVille", a gamified experience launched in 2011 by the game developer Zynga to provide users with its privacy policy in form of a game, where users were rewarded of the relevant information when completing all the steps of the game. However, such a privacy policy was removed in 2017.

[70] J Hamari, T Nousiainen, 'Why do teachers use game-based learning technologies? The role of individual and institutional ICT readiness' (2015) The 48th Hawaii International Conference on System Sciences, 682–691.

world with avatars, and information is provided step by step during the game through entertaining and appealing mechanisms, e.g. in form of points or rewards. This method still needs further investigation, but several benefits have already been identified, given that it makes the notice much more attractive (especially for young people) and motivates data subjects to read it.[71] Clearly the virtual environment cannot completely replace the plain text that in any case should be provided at data subjects' request with full information.

Conclusions.

In the previous sections I have analysed some of the most recurring data protection communication hurdles that data controllers face when designing and displaying their privacy policy. As seen, such hurdles give rise to communication failures that, in the end, water down the substance of the principle of transparency set forth by the GDPR. Indeed, data controllers are more interested in a formalistic application of the information duties imposed by the Regulation, while do not pay enough attention to the function of such duties, that is to empower data subjects and allow them to maintain full control over their personal data and exercise their rights. In practice, the information duties imposed by Arts. 13 and 14 GDPR result in long and complex documents written with legal technical terms and hardly understandable by the layman. The consequence is that data subjects do not really read privacy notices and, therefore, are completely unaware of the processing of their personal data and unable to take meaningful decisions about it.

However, it seems that things are slowly changing. Indeed, today's digital innovation is embracing all the fields of knowledge, including law. This entails, on the one hand, that users are gaining more awareness about both the risks posed by the digital environment and their rights, with the consequence that no longer accept that companies process their personal data in an opaque and confusing way (the WhatsApp case referred to in the introduction confirms that). On the other hand, lawyers themselves (or, at least, many of them) start to understand that the legal system needs to change in accordance with the outside world. Indeed, the current digital transformation is not just technological but social and cultural as well and imposes changes also in lawyers' mindset and perspective.

In particular, for the legal system this means rethinking the way lawyers interact with other stakeholders (clients, companies, and the society as a whole): while, so far, law has always been seen as austere and distant from people – and this is reflected by the use of "legalese" to write legal documents – now it should become closer and more accessible. Herein, more emphasis should be placed on communication and design and a more interdisciplinary

[71] See for example RJ Baxter, DK Holderness, DA Wood, 'Applying basic gamification techniques to IT compliance training: Evidence from the lab and field' (2016) 30(3) Journal of Information Systems, 119–133; E Dincelli, I Chengalur-Smith, 'Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling' (2020) 29(6) European Journal of Information Systems, 669-687.

approach should be adopted.

Design should not be considered just as aesthetics and graphics, but it may become a tool to improve the disclosure and communication of legal products, so that they can effectively reach the intended recipients. To that end lawyers should work together with computer technicians, IT experts and designers to offer a service that can actually meet needs and expectations of different targets of users. Rather than designed by lawyers for lawyers, law should be designed for its actual recipients.

In particular, in the field of data protection and privacy notices, several design patterns have been examined that can help practitioners to make the privacy policy more attractive and understandable to data subjects. Many of them, like icons and layered notices, are already in place and are gaining much attention in the data protection panorama. Others, like cartoons and gamified experiences, still need more investigation to ensure that the relevant information is provided in an adequate manner, but may lead to significant benefits, especially to deliver the required information to young users.

As for the forthcoming years, legal design is expected to play a crucial role in the development of transparent and effective privacy notices and, thus, to put data subjects at the centre of the processing of personal data. Further design patterns will likely be realised based on an interdisciplinary approach in order to make privacy notices more tailored on the intended recipients and, in such a way, more coherent with their substantial purpose.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Derechos digitales en México.
Digital rights in Mexico.

JAVIER MARTÍNEZ CRUZ
Commissioner of the institute of transparency, access to public information and protection of personal data of the state of Mexico and Municipalities

Abstract

La Carta de los Derechos Fundamentales de la Unión Europea prevé el derecho de protección de datos personales; para ello, el Reglamento General de Protección de Datos establece que el tratamiento debe estar concebido para servir a la humanidad y brinda la posibilidad de que los Estados miembros adopten disposiciones nacionales para especificar un mayor grado de aplicación; por tanto, España en su Constitución refiere la obligación de garantizar el honor y la intimidad personal y familiar de los ciudadanos, destacando la emisión de la Ley Orgánica 3/2018 del 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, considerando el aumento exponencial del tratamiento automatizado de datos personales ante la conectividad a internet en el ámbito de nuestras actividades profesionales, educativas, económicas y sociales. En este contexto, resulta necesario el reconocimiento y regulación de los derechos digitales en México, a partir de la modificación y/o adición en la normatividad aplicable en materia de protección de datos personales y el fortalecimiento de los órganos encargados de garantizar este derecho, reconocido expresamente en la Constitución Federal.

The Charter of Fundamental Rights of the European Union provides for the right to protect personal data; For this, the General Data Protection Regulation establishes that the processing must be designed to serve humanity and provides the possibility for member states to adopt national provisions to specify a greater degree of application; Therefore, Spain in its Constitution refers to the obligation to guarantee the honor and personal and family privacy of citizens, highlighting the issuance of the Organic Law on Protection of Personal Data and Guarantee of Digital Rights, considering the exponential increase in automated processing of personal data in the face of internet connectivity in the field of our professional, educational, economic and social activities. In this context, it is necessary to recognize and regulate digital rights in Mexico, based on the modification and / or addition of the applicable regulations regarding the protection of personal data and the strengthening of the bodies in charge of guaranteeing this right, recognized expressly in the Federal Constitution.

Palabras clave: Protección de datos personales; derechos digitales; internet; tecnologías de información y comunicación.

Keywords: Protection of personal data; digital rights; internet; information and communication technologies.

Introduction.

En México se reconoce el derecho de protección de datos personales en la Constitución Política de los Estados Unidos Mexicanos como un derecho humano; sin embargo, resulta necesario el reconocimiento de este derecho en el entorno digital, a fin de garantizar otros derechos como la libertad de expresión, el acceso a la información pública, la educación digital y el acceso universal a internet, para erradicar la brecha digital y garantizar el acceso a internet en todo el país, específicamente el acceso a las tecnologías de la información y comunicación, destacando la Carta de Derechos Humanos y Principios para Internet de la Organización de las Naciones Unidas que contempla 10 derechos para garantizar la interacción segura, libre y respetuosa en internet.

México cuenta con un marco normativo en materia de protección de datos personales en el ámbito público y privado que tienen como objetivo establecer las bases, principios y procedimientos para tutelar y garantizar este derecho, a partir de la distribución de competencias de los organismos garantes, la observancia de principios y deberes previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; así como, establecer procedimientos sencillos y expeditos para el ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad de datos personales, precisando que cada vez hay más personas interactuando en el mundo digital, considerando el fácil acceso a plataformas tecnológicas que recaban información de carácter personal para la prestación de un servicio, la compra de un producto, o bien, el desarrollo de actividades profesionales o académicas. Por tanto, resulta fundamental regular los derechos en el contexto digital como una extensión al derecho de protección de datos personales que se encuentra previsto en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.

En el ámbito internacional, Europa constituye un marco de referencia en la regulación del derecho de protección de datos personales en el Reglamento General de Protección de Datos Personales vigente desde el año 2018, destacando que en el mismo año, España emitió la Ley Orgánica 3/2018 del 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales que contempla un total de 17 derechos digitales, los cuales reconocen

los derechos y libertades consagrados en la Constitución Española y los Tratados internacionales de los que España es parte y que resultan aplicables en internet, donde la sociedad de la información y los proveedores de servicios deben contribuir a la aplicación de dicha normatividad. En tal virtud, el objetivo del presente artículo consiste en analizar la legislación española como un referente para la regulación de los derechos digitales en México como una extensión del derecho fundamental de protección de datos personales.

1. Derechos digitales. Regulación necesaria en México.

El uso de internet ha generado un cambio en la sociedad, al contribuir en la aplicación de nuevas formas de comunicarnos con el exterior para trabajar de una manera más rápida y eficiente, con la creación de nuevas técnicas de educación e incluso el cambio en la manera de hacer negocios. A partir de ello, se comenzaron a desarrollar las tecnologías de información y comunicación, mismas que son usadas por las personas de manera individual y por las llamadas sociedades de la información, que a su vez han generado cambios en la organización social y productiva.

Estas tecnologías comenzaron con la radio, seguidas por el televisor, el teléfono análogo y posteriormente, las computadoras personales, teléfonos y otros dispositivos inteligentes que han transformado de manera significativa la manera en que nos comunicamos, ya que permiten digitalizar miles de millones de datos en tiempo real y en cualquier parte del mundo.

Este nuevo paradigma tecnológico en la sociedad de la información implica una capacidad masiva de captación, comunicación, almacenamiento y procesamiento veloz de la información y conduce a una profunda reorganización económica y social[1]; por lo tanto, nos encontramos ante un presente que se mueve en un entorno tecnológico; es decir, estamos frente a una cuarta revolución industrial, donde el núcleo es la tecnología de la información y la conexión digital mediante el internet.

Las tecnologías de la información y comunicación han tenido un incremento exponencial en los últimos años, ante el desarrollo tecnológico y la inclusión de nuevas tecnologías como el machine learning, el big data o la inteligencia artificial, considerando que para el año 2019 el 57% de la población mundial eran usuarios de internet, de los cuales el 67% se conectan a través de dispositivos móviles, cuyo uso más frecuentes es la navegación en redes sociales[2]; sin embargo, esta conexión digital conlleva un riesgo a la privacidad, la reputación y a la dignidad del ser humano, debido a las grandes cantidades de datos personales que se recolectan de manera digital, donde las personas

[1] González, Daniela y Ortiz, Laura. "La medición, a través de los censos de población y vivienda, del acceso y uso personal y desde el hogar a las tecnologías de la información y las comunicaciones". Comisión Económica para América Latina y el Caribe (CEPAL) y Centro Latinoamericano y Caribeño de Demografía (CELADE). Notas de Población Año XXXVII, No. 92. Santiago de Chile. 2011. Pág. 47-90. Recuperado el 21 de mayo de 2021 de https://repositorio.cepal.org/bitstream/handle/11362/12880/np92047090_es.pdf?sequence=1&isAllowed=y

[2] Informe Digital 2019. "Todos los datos y tendencias que necesitas para entender los comportamientos en internet, redes sociales, móvil y comercio electrónico en 2019". We are social y Hootsuite. España. 2019.

corren el riesgo de perder el control sobre su información personal, principalmente de los datos que pertenecen a su esfera más íntima; es decir, los datos personales sensibles como los datos relativos a la salud, genéticos y biométricos.

En el caso de México, el uso de internet ha crecido en los últimos años, para el año 2018 se presentó un incremento del 4.3% comparado con el año 2017; es decir, para el año 2018 había casi 83 millones de internautas. Por otro lado, la población internauta mexicana con mayor uso de internet es la que se mantiene en edades de entre los 18 a 34 años de edad, representando un 40% de la población, haciendo uso para su conexión de dispositivos como Smartphone o teléfonos inteligentes y lap tops, representando un 92% y 76% de regularidad de uso respectivamente; además, el 82% de la población internauta del estado mexicano hace uso de sus dispositivos inteligentes para navegar en redes sociales y el 78% para enviar y recibir mensajes instantáneos[3].

Al navegar en internet se proporcionan datos personales, ya sea para registro en plataformas o sitios web, realizar pagos por la contratación de algún servicio o la adquisición de un producto, seguimiento o participación en foros, conferencias o seminarios, el teletrabajo o la telemedicina. En México, el 48% de la población internauta usa su tarjeta de crédito para realizar pagos, de los cuales el 51% considera que usarla resulta más cómodo, sencillo y práctico. En este contexto, se puede identificar que en las actividades que realizamos, es muy común proporcionar información personal como el nombre, domicilio, teléfono y datos bancarios en el mundo digital, aunado a que de acuerdo a la Asociación de Internet, en México el 67% de la población internauta considera que pasa conectado las 24 horas del día y que el promedio el total de los usuarios pasa 8 horas con 20 minutos conectados de manera continua, lo que se traduce en un intercambio masivo de información en el ciberespacio[4].

Por lo anterior, es importante delimitar el derecho de protección de datos personales ante el uso de la información que circula en el universo digital, sin impedir el uso de las tecnologías y el acceso a internet, a fin de que las personas proporcionen su información personal con la garantía de que las instituciones públicas y privadas cumplan con las disposiciones aplicables en la materia; así mismo, es importante mencionar que en el caso de las relaciones comerciales, la tecnología tiene un papel importante en la prestación de bienes y servicios, precisando que en México de acuerdo al Instituto Nacional de Estadística y Geografía (INEGI) el comercio digital en el año 2018 representó el 5% del Producto Interno Bruto (PIB), lo que implica el tratamiento de datos personales, especialmente el nombre, domicilio, teléfono y datos patrimoniales como el número de cuenta, número de tarjeta o la clave interbancaria para realizar transacciones electrónicas en el contexto de la economía digital[5].

---

[3] Asociación de Internet MX. Estadística Digital. "15° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018. Movilidad en el Usuario de Internet Mexicano". México. 31 de julio de 2019.
[4] Ídem.
[5] Estadística Digital. "El INEGI da a conocer resultados del valor agregado bruto del comercio electrónico 2018". Instituto Nacional de Estadística y Geografía. Comunicado de Prensa Número 69/20. 12 de febrero de 2020. Recuperado el 22 de mayo de 2021 de https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/vabce2018.pdf

A partir de ello, en México surge la necesidad de reconocer los derechos digitales; es decir, la protección de las personas ante el uso de las tecnologías que permitan una garantía de protección de la personalidad y la dignidad humana. En México, la regulación de la protección de datos personales en el sector privado se efectúa a través de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley Federal); mientras que, en el sector público se cuenta con la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (Ley General) que tienen como objetivo garantizar el derecho que tiene toda persona a la protección de sus datos personales, derecho que se encuentra reconocido en la Constitución Política de los Estados Unidos Mexicanos (Constitución Federal).

En este orden de ideas, México cuenta con un marco jurídico sólido en materia de protección de datos personales, destacando la conformación del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Sistema Nacional de Transparencia), como un espacio para construir una política pública que tiene por objeto garantizar el efectivo ejercicio y respeto del derecho de protección de datos personales, a fin de promover y fomentar la educación y cultura de este derecho en el territorio nacional, precisando que dicho sistema se encuentra integrado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y los organismos garantes de las Entidades Federativas, que en su conjunto realizan actividades coordinadas para implementar procedimientos, políticas y mecanismos que fortalecen el ejercicio del derecho de protección de datos personales.

De igual manera, es primordial mencionar que México forma parte del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter personal (Convenio 108) y su protocolo adicional relativo a las Autoridades de Control y los Flujos Transfronterizos de Datos, con el objetivo de fortalecer el marco jurídico en materia de protección de datos personales, promover la cooperación internacional y garantizar un nivel adecuado de protección en el flujo transfronterizo de datos con los países miembros de la Unión Europea[6]; firmó el Tratado entre los Estados Unidos Mexicanos, Estados Unidos de América y Canadá (T-MEC) que aunque tienen fines meramente comerciales, prevé aspectos importantes relativos a servicios financieros, telecomunicaciones, comercio digital y derechos de propiedad intelectual[7]; así mismo, participa en el Sistema de Normas de Privacidad Transfronteriza (CBPR) del Foro de Cooperación Económica de Asia Pacífico (APEC) que consiste en un sistema para garantizar que la información personal ante el flujo transfronterizo de datos debe estar protegida bajo los estándares del marco de privacidad de APEC.

Por su parte, Europa se caracteriza por reconocer el derecho de protección de datos personales como un derecho fundamental; para ello, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016

[6] Decreto Promulgatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de mil novecientos ochenta y uno. Diario Oficial de la Federación. México. 28 de septiembre de 2018.

[7] Decreto Promulgatorio del Protocolo por el que se Sustituye el Tratado de Libre Comercio de América del Norte por el Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá. Diario Oficial de la Federación. 29 de junio de 2020.

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos Personales) en el considerando cuarto señala: "El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad" [8]; así mismo, el artículo tercero refiere la aplicación del Reglamento cuando las actividades del tratamiento se relacionen con la oferta de bienes o servicios a interesados dentro o fuera de la Unión Europea, independientemente de que se requiera un pago.

En tal virtud, las relaciones comerciales y en general, la navegación en internet debe garantizar el derecho fundamental de protección de datos personales, ya que, aun cuando la mayoría de las transferencias de datos personales se realizan con fines económicos, existen actividades como la educación digital que requiere especial atención ante la conectividad de menores de edad que interactúan en el mundo digital para llevar a cabo sus actividades académicas, destacando que es responsabilidad del Estado implementar políticas públicas inclusivas que garanticen una navegación segura en internet, o bien, el ejercicio del derecho de portabilidad ante el tratamiento automatizado de datos personales, con la implementación de medidas técnicas que permitan obtener una copia de la información personal o la transferencia de dicha información entre los responsables del tratamiento.

Ahora bien, como se mencionó anteriormente, en México la regulación en materia de protección de datos personales se aplica en el sector público y privado, destacando que en el sector público se prevé el derecho de portabilidad que consiste en el tratamiento de datos personales por vía electrónica; no obstante, en dicha normatividad no se encuentra prevista alguna otra disposición que permita diferenciar la aplicación en el entorno físico y el entorno digital; precisando que de los países de América Latina, México es el país que más ha avanzado en ampliar la conectividad a internet, a partir de la reforma al artículo sexto Constitucional que establece: "El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet"[9].

De igual manera, el Plan Nacional de Desarrollo 2019 – 2014 prevé la cobertura de internet en todo el país, mediante la instalación de internet inalámbrico en todo el país para ofrecer a toda la población la conexión en carretera, plazas públicas, centros de salud, hospitales, escuelas y espacios comunitarios, a fin de combatir la marginación y la pobreza para la integración

[8] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). 27 de abril de 2016. Diario Oficial de la Unión Europea. Europa: Parlamento Europeo. 2016. Considerando 4.

[9] Constitución Política de los Estados Unidos Mexicanos. (17 de mayo de 2021). Diario Oficial de la Federación. México: Cámara de Diputados del H. Congreso de la Unión. Artículo 6.

de las zonas reprimidas en las actividades productivas[10].

En tal virtud, México se ha posicionado como un país que reconoce el derecho de protección de datos personales como un derecho humano y, por ende, como una nación que implementa mecanismos y procedimientos para el pleno ejercicio de este derecho; sin embargo, en el entorno digital resulta necesario el reconocimiento de ciertos derechos, considerando lo previsto en la Carta de Derechos Humanos y Principios para Internet emitida por la ONU, un instrumento de índole internacional que está basada en la Declaración Universal de los Derechos Humanos, la cual propone los derechos siguientes: universalidad e igualdad, derechos y justicia social, accesibilidad, confidencialidad y protección de datos, vida, libertad y seguridad, diversidad, igualdad, normas y reglamento y gobierno[11]; derechos que en su conjunto, constituyen medidas que permiten que el internet funcione de manera que cumpla y respete los derechos humanos, destacando la intervención de instituciones públicas y privadas.

La Carta objeto de análisis considera aspectos de suma importancia en materia de protección de datos personales, como el derecho que tiene toda persona a la privacidad online, la autodeterminación informativa y el deber de ser informado del tratamiento al que serán sometidos sus datos personales; por ello, resulta necesaria la regulación de los derechos digitales en México, considerando que en el ámbito internacional, la Declaración Universal de los Derechos Humanos en su artículo 1, manifiesta: "Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros"[12].

En este sentido, los seres humanos desde que nacen tienen adherida su dignidad, un bien que debe protegerse en todo momento, aun cuando la sociedad evolucione y su entorno manifieste cambios con el paso del tiempo, resultando necesaria la evolución de los derechos para atender las necesidades políticas, económicas y sociales que se presenten en un tiempo y lugar determinado. Es así, que al desenvolvernos en un ambiente digital, se comience a hablar de derechos digitales, atendiendo a que toda la información que fluye en el ciberespacio es manejada por humanos, destacando que aun cuando la información esta automatizada, las instrucciones son creadas por humanos y, por ende, resulta fundamental establecer límites en el tratamiento de datos personales en el entorno digital, donde cada vez hay más personas que se desenvuelven en el intercambio de información para llevar a cabo sus actividades profesionales, académicas, económicas y sociales, basta con tener un dispositivo inteligente y acceso a internet para intercambiar mensajes, fotos, videos y cualquier contenido digital.

Por lo tanto, los derechos digitales son derechos que pretenden proteger a las personas en el entorno digital, a fin de evitar que las personas sufran alguna afectación en su persona, imagen, dignidad y seguridad, sin impedir que las personas tengan derecho a expresarse de una manera respetuosa; por tanto,

[10] Plan Nacional de Desarrollo 2019 – 2024. Diario Oficial de la Federación. 12 de julio de 2019.
[11] Carta de derechos humanos y principios para internet. 1ra. Edición. Organización de las Naciones Unidas. Foro para la Gobernanza de Internet. 2015. Recuperado el 21 de mayo de 2021 de https://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf
[12] Declaración Universal de Derechos Humanos. Asamblea General de la Organización de las Naciones Unidas. 10 de diciembre de 1948. Artículo 1.

los derechos digitales están relacionados con otros derechos como el derecho a la privacidad, el derecho a la intimidad, el derecho a la imagen, el derecho a la libertad de expresión, derecho al internet y el derecho a la desconexión digital.

En el caso específico de Europa, la Carta de los Derechos Fundamentales de la Unión Europea en los artículos 7 y 8 refiere: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan"[13]. Así mismo, la Constitución de España precisa en el artículo 18.4 que: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[14]; para lo cual, en el año 2018 España emite la Ley Orgánica 3/2018 del 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (Ley Orgánica), que modifica las exigencias en el tratamiento de datos personales, buscando adaptar la legislación española a la normativa europea en temas de protección de datos personales regida por el Reglamento General de Protección de Datos, cuya principal novedad es la inclusión del principio de responsabilidad proactiva.

Teniendo esto en cuenta, México tiene la obligación de garantizar el pleno ejercicio de los derechos digitales, específicamente lo relativo a la protección de datos personales en el contexto digital, de conformidad con los instrumentos internacionales de los que forma parte, como el Convenio 108 y su protocolo adicional que lo reconocen como un derecho fundamental o el T-MEC que a pesar de tener finalidades de carácter económico, garantizan aspectos relativos al uso de datos personales, atendiendo a lo previsto en la Constitución Federal, Leyes y Lineamientos que prevén lo relativo a principios, deberes, derechos, medios de impugnación, transferencias nacionales e internacionales, medidas de seguridad y violaciones a la seguridad de los datos personales.

2. El reconocimiento de los derechos digitales en España como un referente para su regulación en México.

Para efectos del presente estudio, se toma como referencia la Ley Orgánica de España, la cual prevé los derechos digitales siguientes: neutralidad de internet, acceso universal a internet, seguridad digital, educación digital, protección de los menores en internet, rectificación en internet, actualización de informaciones en medios de comunicación digitales, intimidad y uso de dispositivos digitales en el ámbito laboral, desconexión digital en el ámbito laboral, intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo, intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, derechos digitales en la negociación colectiva, protección de datos de los menores en internet, derecho al olvido en búsquedas de internet, derecho al olvido en servicios de redes sociales y servicios equivalentes, derecho de portabilidad en servicios de redes sociales y

[13] Carta de los Derechos Fundamentales de la Unión Europea. Diario Oficial de las Comunidades Europeas. 18 de diciembre de 2000. Artículos 7 y 8.
[14] Constitución Española. Boletín Oficial del Estado. España. 29 de diciembre de 1978. Artículo 18.4.

servicios equivalentes y el derecho al testamento digital[15].

En este orden de ideas, en México resulta fundamental considerar el reconocimiento del derecho digital de neutralidad de internet, con la finalidad de que los proveedores de servicios como Telmex, Izzi, Megaclabe, Totalplay o Dish proporcionen ofertas transparentes a los usuarios, para brindar servicios eficientes que establezcan condiciones contractuales o prácticas comerciales que no discriminen o limiten directa o indirectamente por motivos técnicos, geográficos o económicos.

En el caso del derecho digital de acceso universal a internet, en México se encuentra contemplado en el artículo sexto de la Constitución Federal; sin embargo, resulta innecesario su reconocimiento como extensión al derecho de protección de datos personales, considerando que el Plan Nacional de Desarrollo 2019 – 2024 prevé la cobertura de internet en todo el país, independientemente de la condición social, económica y geográfica, a fin de que el acceso a internet sea de calidad y garantice condiciones de igualdad en la contratación del servicio[16]. Así mismo, el Programa Nacional de Protección de Datos Personales (PRONADATOS)[17] en el Eje 1 denominado "Educación y cultura de protección de datos personales en la sociedad mexicana" prevé el acompañamiento a los usuarios en el cierre de la brecha digital en materia de protección de datos personales, atendiendo a que el proceso de integración tecnológica trae consigo beneficios y riesgos en el tratamiento de la información, ante el uso de las nuevas tecnologías de información y comunicación, con la finalidad de brindar a los usuarios medidas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de los datos personales; además, en el Eje 2 identificado como "Ejercicio de los derechos ARCO y de portabilidad" refiere el acompañamiento a los usuarios digitales en el cierre de la brecha digital para el ejercicio de los derechos ARCO y el desarrollo de sus herramientas de facilitación[18].

Por lo que corresponde al derecho a la seguridad digital, la Ley Orgánica de España refiere: "Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos"[19]. En México el artículo 16 Constitucional establece que "Las comunicaciones son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de

[15] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Boletín Oficial del Estado. Gobierno de España. 6 de diciembre de 2018. Artículos 79 al 96.
[16] Plan Nacional de Desarrollo 2019 – 2024. Diario Oficial de la Federación. 12 de julio de 2019.
[17] En términos del artículo 12 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Sistema Nacional de Transparencia tiene como objetivo diseñar, ejecutar y evaluar el Programa Nacional de Protección de Datos Personales que defina la política pública.
[18] Acuerdo mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales. Diario Oficial de la Federación. 26 de enero de 2018.
[19] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Boletín Oficial del Estado. Gobierno de España. 6 de diciembre de 2018. Artículo 82.

confidencialidad que establezca la ley"[20]. Para ello, la Ley General en el artículo 31 señala que los responsables deben establecer y mantener medidas de seguridad físicas, técnicas y administrativas para la protección de datos personales, a fin de evitar cualquier daño, pérdida, alteración, destrucción, acceso o tratamiento no autorizado; así como, garantizar su confidencialidad, integridad y disponibilidad[21]. Por tanto, en México se reconoce este derecho, no precisamente como un derecho digital; pero, sí como una garantía en el tratamiento y seguridad de los datos personales.

No obstante a lo anterior, el derecho a la educación digital debe ser reconocido en México considerando que el PRONADATOS en el Eje 1 establece la inclusión de una cultura de protección de datos personales en los programas educativos de distintos niveles, a fin de sensibilizar y concientizar a la población; además, de desarrollar profesionales y especialistas en la materia que cumplan con un perfil adecuado para dar cumplimiento a los principios, deberes y obligaciones que establece la Ley General. Así mismo, el Eje 2 prevé la inclusión del tema de derechos ARCO y portabilidad en los programas educativos, lo cual implica la coordinación con las instituciones educativas[22].

Asimismo, en lo que corresponde a este derecho, se debe considerar que la mayoría de los que interactúan en internet con fines educativos son menores de edad y, por ende, se debe garantizar que el uso de los medios digitales sea seguro y no se incurra en conductas que puedan afectar arbitrariamente la privacidad de los usuarios, mediante la aplicación de medidas que aseguren la protección de sus datos personales en el entorno digital, ponderando la importancia de implementar políticas públicas que incluyan la intervención de profesores y padres de familia para la supervisión de los menores en la red, a fin de implementar planes de estudio con un enfoque de derechos humanos que otorgue garantías para la protección de la intimidad personal y familiar.

Ahora bien, en lo que corresponde a la protección de menores en internet, específicamente a la protección de sus datos personales, es un derecho digital que debe reconocerse en México, ya que, aun cuando la normatividad prevé diversos aspectos para garantizar la protección de los menores, resulta indispensable la coordinación entre padres, instituciones educativas y organismos garantes, para promover una cultura de protección de protección de datos personales entre los niños, niñas y jóvenes, a fin de garantizar el desarrollo de su personalidad, preservar su dignidad y el respeto a sus derechos fundamentales. La regulación de este derecho debe incluir aspectos como la difusión de imágenes o datos personales de menores en redes sociales y servicios de la sociedad de la información como operadores de telecomunicaciones, proveedores de acceso a internet o motores de búsqueda, con el objetivo de garantizar la protección del interés superior del menor y sus derechos fundamentales.

En este sentido, se puede tomar como referencia la Carta de los derechos digitales de los niños, niñas y adolescentes que emitió la Fundación "Ayuda a

[20] Constitución Política de los Estados Unidos Mexicanos. (17 de mayo de 2021). Diario Oficial de la Federación. México: Cámara de Diputados del H. Congreso de la Unión. Artículo 16.
[21] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Diario Oficial de la Federación. 26 de enero de 2017. Artículo 31.
[22] Acuerdo mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales. Diario Oficial de la Federación. 26 de enero de 2018.

Niños y Adolescentes en Riesgo" (ANAR)[23], la cual contempla aspectos como el interés superior del menor en el entorno digital y su protección frente a contenidos y dispositivos que puedan afectar su desarrollo físico y mental, asegurar su privacidad, ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), limitación del tratamiento y portabilidad, a través de sus representantes legales; así como, la posibilidad de ejercer el derecho al olvido en búsquedas de internet y en redes sociales, a fin de que puedan borrar su huella digital[24].

España establece como derecho digital, la rectificación en internet, para el caso de México resulta procedente el reconocimiento de los derechos ARCO en el entorno digital, para que los titulares puedan ejercer sus derechos ante los responsables de las redes sociales, plataformas y aplicaciones electrónicas, sitios web o cualquier otro medio digital que utilice datos personales. La posibilidad de ejercer los derechos ARCO en internet, garantizará a los usuarios su derecho a la imagen, el honor, la intimidad personal y familiar, la autodeterminación informativa y el derecho a comunicar y recibir información, de conformidad con las disposiciones previstas en la Ley Federal, la Ley General y demás normatividad aplicable, especialmente en lo relativo a requisitos, plazos y procedimientos.

De igual manera, el derecho a la actualización de información en medios de comunicación digitales, consiste en que toda persona puede solicitar a los medios de comunicación digitales, la inclusión de un aviso de actualización en las noticias que le conciernen, atendiendo a que la noticia original le causa un perjuicio ya que se refieren a actuaciones policiales o judiciales; es decir, la actualización de la información implica la publicación de decisiones judiciales posteriores que benefician al titular de los datos personales. En este sentido, en México debería reconocerse expresamente este derecho, ya que implica que los responsables y los organismos garantes realicen un ejercicio de la ponderación del derecho de protección de datos personales y el interés público de conocer la información, bajo la aplicación del test de proporcionalidad que se conforma de tres elementos, idoneidad, necesidad y proporcionalidad en sentido estricto.

En el ámbito laboral, en México sería también preciso establecer el derecho a la intimidad ante el uso de dispositivos digitales, videovigilancia, grabación de sonidos, geolocalización y desconexión digital, que comprende la protección de los trabajadores cuando utilizan los dispositivos para el desarrollo de sus actividades laborales; para ello, los patrones deben establecer protocolos o políticas que dispongan lo relativo a la utilización de dispositivos digitales, que tengan por objeto controlar el cumplimiento de sus obligaciones laborales, de conformidad con lo previsto en la Constitución Federal, la Ley Federal del Trabajo y la Ley General en lo que corresponde al cumplimiento de los deberes de integridad, disponibilidad y confidencialidad de los datos personales; así

[23] La Fundación ANAR es una organización sin ánimo de lucro, cuyos orígenes se remontan a 1970 y se dedica a la promoción y defensa de los derechos de los niños y adolescentes en situación de riesgo y desamparo mediante el desarrollo de proyectos tanto en España y Latinoamérica en el marco de la Convención de los Derechos del Niño de la Organización de las Naciones Unidas.

[24] Carta de los derechos digitales de los niños, niñas y adolescentes. Fundación Ayuda a Niños y Adolescentes en Riesgo (ANAR). Recuperado el 22 de mayo de 2021 de https://www.anar.org/wp-content/uploads/2019/11/Carta-Derechos-Digitales_2811.pdf.

mismo, dichas políticas deberán determinar los periodos en que los trabajadores podrán utilizar los dispositivos digitales para fines privados.

Ahora bien, como lo refiere la Ley Orgánica de España, en México el uso de dispositivos de videovigilancia y grabación de sonidos en el trabajo, debería atender las disposiciones en materia de protección de datos personales, debido a que la Ley Federal del Trabajo establece que solo se podrán utilizar cámaras y micrófonos para supervisar el trabajo en situaciones extraordinarias o cuando así lo requiera la modalidad del teletrabajo[25], precisando que su uso debe realizarse únicamente para ejercer funciones de control de los trabajadores; además, los responsables del tratamiento deben informar a los trabajadores sobre la implementación de dichos dispositivos; cabe destacar, que la instalación de sistemas de videovigilancia y grabación de sonidos no debe admitirse en espacios destinados al descanso y esparcimiento de los trabajadores como sanitarios, vestidores y comedores.

De igual manera, la utilización de sistemas de geolocalización se podrá realizar cuando el giro comercial de las actividades del responsable sean relativas al trasporte de personas, bienes o mercancías, o bien, exista un riesgo para la seguridad de las instalaciones, bienes o personas que se encuentran en el centro de trabajo, con el objetivo de ejercer funciones de control de los trabajadores, destacando que la implementación de estos sistemas debe obedecer a una expectativa razonable de privacidad. En el caso de la desconexión digital, la Ley Federal del Trabajo prevé que los patrones tienen que respetar el derecho a la desconexión de los trabajadores en la modalidad de teletrabajo al término de la jornada laboral[26], para que puedan disfrutar su tiempo de descanso y vacaciones, a fin de respetar su intimidad personal y familiar; para ello, en México se tendrán que establecer políticas públicas para delimitar el ejercicio de este derecho e implementar acciones concretas ante el uso de herramientas tecnológicas, bajo una perspectiva de derechos humanos.

En España se regulan los derechos digitales en la negociación colectiva, que consisten en que los convenios colectivos pueden establecer garantías adicionales de los derechos y libertades relacionadas con el tratamiento de datos personales de los trabajadores y la salvaguarda de los derechos digitales en el ámbito laboral. En México, la regulación de los contratos colectivos de trabajo se establece en la Constitución Federal y la Ley Federal del Trabajo; para lo cual, los responsables del tratamiento de datos personales deben dar cumplimiento a la Ley General y la Ley Federal. En tal virtud, en México ya se cuenta con una regulación específica aplicable a la negociación colectiva; por tanto, en el ámbito laboral únicamente se requiere el reconocimiento del derecho a la intimidad ante el uso de dispositivos digitales, videovigilancia, grabación de sonidos, geolocalización y desconexión digital; es decir, cuestiones inherentes estrictamente al tratamiento de los datos personales.

Ahora bien, el Reglamento General de Protección de Datos prevé el derecho de supresión mejor conocido como derecho al olvido; para ello, los responsables están obligados a suprimir los datos personales en los casos siguientes: cuando los datos personales ya no son necesarios para los fines para los que fueron recabados, cuando los interesados retiren su consentimiento, o

[25] Ley Federal del Trabajo. Diario Oficial de la Federación. México. (23 de abril de 2021). Artículo 330-I.
[26] Ibídem, artículo 330-E.

bien, cuando se opongan al tratamiento y no existen motivos legítimos para llevarlo a cabo, cuando el tratamiento de los datos es ilícito, cuando los datos personales deban suprimirse para el cumplimiento de una obligación legal o cuando se obtengan por la oferta de servicios de la sociedad de la información[27]. En este sentido, la Ley Orgánica de España establece como derechos digitales, el derecho al olvido en búsquedas de internet y el derecho al olvido en servicios de redes sociales y servicios equivalentes[28].

En México no se encuentra reconocido explícitamente el derecho al olvido; sin embargo, la Ley General establece en el artículo 46 lo siguiente: "El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en posesión y dejen de ser tratados por este último"[29]. En este sentido, resulta necesario el reconocimiento del derecho al olvido, considerando que aplica específicamente a los datos personales automatizados, a fin de que toda persona solicite ante los motores de búsqueda, la eliminación de la información obtenida en los resultados y enlaces al incluir su nombre, principalmente cuando los datos sean inadecuados, inexactos, excesivos o se encuentren desactualizados; o bien, cuando requieran la eliminación de su información personal ante los responsables de redes sociales, atendiendo a los fines para los cuales se recabaron los datos y las políticas de privacidad que implementan los responsables del tratamiento.

Por otro lado, en Europa, el derecho de portabilidad se encuentra regulado en el artículo 20 del Reglamento General de Protección de Datos y en España, la Ley Orgánica en el artículo 95 establece el derecho de portabilidad en servicios de redes sociales y servicios equivalentes, donde los usuarios tienen derecho a recibir y transmitir la información que se proporcionó a los prestadores de dichos servicios, siempre que sea técnicamente posible. De igual manera, en México la Ley General en el artículo 57 establece: "Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales"[30].

Asimismo, el Sistema Nacional de Transparencia emitió los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad

[27] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). 27 de abril de 2016. Diario Oficial de la Unión Europea. Europa: Parlamento Europeo. 2016. Artículo 17.

[28] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Boletín Oficial del Estado. España. 6 de diciembre de 2018. Artículos 93 y 94.

[29] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Diario Oficial de la Federación. México. 26 de enero de 2017. Artículo 46.

[30] Ibídem, artículo 57.

de datos personales, los cuales establecen el objeto, alcance, procedencia, reglas específicas, normas técnicas y procedimientos para el ejercicio del derecho de portabilidad, precisando que este derecho se aplica a los datos personales automatizados; es decir, que se encuentren en un formato electrónico que permita su utilización y sea interoperable con otros sistemas informáticos, a fin de que los titulares obtengan una copia de sus datos o se lleve a cabo la transmisión entre responsables, cuando existan las condiciones técnicas para su ejercicio, de conformidad con los requisitos, plazos, condiciones términos y procedimientos establecidos en la Ley General[31].

No obstante a lo anterior, en el sector privado no existe una disposición específica de este derecho en la Ley Federal; sin embargo, el Instituto Federal de Telecomunicaciones emitió reglas de portabilidad numérica que establecen los procesos para que los usuarios puedan ejercer dicho derecho ante los proveedores de servicios de telecomunicaciones conservando su número telefónico, el cual constituye un dato personal que debe protegerse en términos de la Ley Federal y la demás normatividad que resulte aplicable, destacando que la regla 16 establece: "Los Proveedores de Servicios de Telecomunicaciones no podrán establecer condiciones contractuales o prácticas comerciales que discriminen o limiten directa o indirectamente el derecho de los Usuarios a portar su número" [32]; es decir, las reglas de portabilidad tienen una finalidad meramente comercial, debido a que están encaminadas a fomentar una sana competencia entre los proveedores de servicios de telecomunicaciones; por tanto, resulta procedente la modificación de la normatividad mexicana en materia de protección de datos personales en el sector privado, a fin de reconocer el derecho de portabilidad desde un enfoque de derechos humanos que incluya todas las garantías necesarias relativas a requisitos, plazos y procedimientos para su ejercicio.

Bajo este contexto, México cuenta con la regulación del derecho de portabilidad, que se ejerce exclusivamente en el entorno digital y, por ende, como en el caso de la legislación española puede ejercerse en servicios de redes sociales y servicios equivalentes, siempre que sea técnicamente posible, destacando que de acuerdo a su naturaleza es procedente su reconocimiento como un derecho digital en México.

3. La herencia digital como un derecho en México.

El Reglamento General de Protección de Datos en el considerando 27 señala lo siguiente: "El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de datos personales de

[31] Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. Diario Oficial de la Federación. 12 de febrero de 2018.

[32] Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones emite las Reglas de Portabilidad Numérica y modifica el Plan Técnico Fundamental de Numeración, el Plan Técnico Fundamental de Señalización y las especificaciones operativas para la implementación de portabilidad de números geográficos y no geográficos. Diario Oficial de la Federación. México. 12 de noviembre de 2014. Regla 16.

estas"[33]. En este sentido, España en la Ley Orgánica contempla el derecho de testamento digital, que consiste en el acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas; para ello, las personas vinculadas al fallecido podrán acceder a dichos contenidos, siempre y cuando el fallecido no lo hubiere prohibido. Los herederos podrán determinar el mantenimiento o eliminación de los perfiles en redes sociales o servicios equivalentes, a menos que el fallecido hubiera indicado lo contrario o determinara las respectivas instrucciones; para lo cual, dispone que mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones[34].

En este contexto, en México de conformidad con la legislación civil, se establece la figura de la herencia como "la sucesión de todos los bienes del difunto y en todos sus derechos y obligaciones que no se extinguen por la muerte"[35]; sin embargo, no se identifica que dicho marco jurídico, señale alguna disposición específica aplicable en el entorno digital, considerando que las tecnologías de la información y comunicación tienen un impacto constante en el ejercicio del derecho de protección de datos personales, precisando que cada vez hay más personas interactuando en el mundo digital que genera información y contenido personal en diversas plataformas, a través de la activación de cuentas electrónicas a las que acceden con sus datos personales (usuarios y contraseñas); por tanto, es importante reconocer la herencia digital como un derecho, a partir de la implementación de mecanismos que permitan a los usuarios determinar lo relativo a su patrimonio de carácter digital en el momento de su fallecimiento.

Además, como se mencionó previamente, en el ámbito internacional la Organización de las Naciones Unidas emitió la Carta de los Derechos Humanos y Principios de Internet, cuyo objetivo principal consiste en determinar que los derechos y principios deben garantizarse en igualdad de condiciones, tanto en el ámbito físico como virtual; así mismo, es importante resaltar que reconoce la personalidad virtual y la posibilidad de comunicarse de forma anónima en internet, con los mecanismos de cifrado que garanticen que la comunicación sea privada y anónima, destacando el deber que tienen todos los usuarios de internet para respetar y proteger los derechos humanos en el entorno digital.

En México, la Ley Federal resulta aplicable en el sector privado, destacando que dicha normatividad no contempla lo relativo al tratamiento de datos para personas fallecidas; mientras que, en el ámbito público, la Ley General establece que tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico podrá ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), siempre que el titular hubiere expresado fehacientemente su voluntad o que exista un mandato judicial para dicho efecto.

---

[33] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). 27 de abril de 2016. Diario Oficial de la Unión Europea. Europa: Parlamento Europeo. 2016. Considerando 27.

[34] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Boletín Oficial del Estado. España. 6 de diciembre de 2018. Artículo 96.

[35] Código Civil Federal. Diario Oficial de la Federación. México. (11 de enero de 2021). Artículo 1281.

Ahora bien, en el caso del Estado de México, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios (Ley Estatal), prevé en el artículo 106 que el titular puede autorizar dentro de una cláusula del testamento, a las personas que podrán ejercer sus derechos ARCO al momento de su fallecimiento. En este sentido, tanto la Ley General como la Ley Estatal establecen lo siguiente: "La interposición de un recurso de revisión de datos personales concernientes a personas fallecidas, podrá realizarla la persona que acredite un interés jurídico o legítimo"[36].

En este orden de ideas, se debe analizar el interés jurídico y legítimo en términos de la legislación civil y lo relativo en materia de amparo, a fin de contar con los elementos necesarios para determinar quién debe ejercer los derechos en materia de protección de datos personales en el caso de personas fallecidas; para lo cual, se deberán ponderar los derechos que pudieran estar en conflicto en cada caso concreto, como el derecho a la verdad ante la comisión de delitos de lesa humanidad o que implique la violación grave de derechos humanos o el derecho a la salud cuando la persona hubiere fallecido por una enfermedad genética o de transmisión sexual en caso de que las personas que requieran tener acceso sean los hijos, padres o cónyuges, en cualquier caso la ponderación se efectuara a través de la aplicación del test de proporcionalidad (idoneidad, necesidad y proporcionalidad en sentido estricto) que consiste en valorar los medios, objetivos, finalidades, los medios hipotéticos y la evaluación de las posibilidades jurídicas que incluye el análisis de los derechos de conflicto y la colisión de principios.

De igual manera, es importante mencionar un acontecimiento relevante suscitado en Alemania, donde una niña fue arrollada en las vías del tren y sus padres pretendían acceder a su cuenta de una red social, a fin de determinar si se trataba de un accidente o un suicidio; para ello, las autoridades competentes a partir de análisis exhaustivo del asunto, resolvieron la apertura de la cuenta y brindaron el acceso a los padres; dicha sentencia es trascendente debido a que se incorporan aspectos como el secreto a las telecomunicaciones, el respeto a la vida privada, la representación y tutela legal, el patrimonio, la correspondencia y la herencia digital. Además, el asunto funge como un precedente en las políticas de uso de las redes sociales, tal es el caso de Facebook con la configuración de cuenta conmemorativa que tiene como finalidad que los usuarios decidan lo que pasará con su cuenta cuando fallezcan, brindando la opción de eliminar definitivamente de la cuenta, o bien, designar un contacto de legado para que administre el perfil y lo elimine posteriormente, destacando que esta persona podrá fijar publicaciones en el perfil, ver publicaciones, decidir quién puede ver y publicar homenajes, eliminar publicaciones de homenaje, eliminar etiquetas, solicitar la eliminación de la cuenta, descargar una copia de la información compartida mientras la cuenta estaba activa, leer mensajes, eliminar personas de la lista de amigos y enviar nuevas solicitudes de amistad.

En tal virtud, el tratamiento de datos en lo que corresponde a personas fallecidas, representa un gran reto para México, al no contar con un marco normativo que regule los derechos digitales, considerando que el artículo sexto

[36] Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios. Periódico Oficial Gaceta de Gobierno. Estado de México. 30 de mayo de 2017. Artículo 122.

constitucional establece la obligación del Estado para garantizar el derecho de acceso a las tecnologías de información y comunicación y los servicios de banda ancha e internet; por tanto, resulta indispensable generar los mecanismos jurídicos necesarios e idóneos, para la regulación de todo lo concerniente a la herencia digital.

Conclusión.

En la actualidad, el uso de nuevas tecnologías de información y comunicación, la conexión masiva a internet y el impacto de la economía digital en el desarrollo de nuestras actividades diarias, implican el tratamiento de información personal; por tanto, existe un riesgo latente de invasión a la privacidad de los usuarios, que trae consigo la violación de derechos humanos reconocidos en distintos instrumentos internacionales de los que México forma parte; por tanto, los responsables del tratamiento de datos personales deben implementar medidas de seguridad físicas, técnicas y administrativas, a fin de garantizar la integridad, disponibilidad y confidencialidad de la información.

México cuenta con normatividad específica en materia de protección de datos personales, que resulta aplicable tanto en el sector público como privado; además, cuenta con órganos encargados de garantizar este derecho, debido a que tienen atribuciones y funciones para la promoción, fomento y cultura de este derecho en todo el territorio nacional. Asimismo, resulta de suma importancia el reconocimiento internacional de México ante Europa, América del Norte y Asia Pacífico al formar parte del Convenio 108, el T-MEC y ser miembro de la APEC.

En este sentido, Europa es la referencia más importante en la regulación del derecho de protección de datos personales al contar con el Reglamento General de Protección de Datos, destacando que al igual que México lo reconoce como un derecho fundamental en la Constitución Federal; así como, el derecho de acceso a las tecnologías de la información y comunicación e internet, cuyo objetivo del Gobierno Federal es la cobertura de internet en todo el país como lo prevé el Plan Nacional de Desarrollo 2019 – 2014.

Una vez realizado el respectivo análisis y bajo los argumentos y razonamientos vertidos en el presente documento, se concluye que en México se deben reconocer los derechos digitales siguientes:

- Neutralidad de internet. Los proveedores de servicios de internet deben aplicar políticas de competencia transparencia, a fin de brindar servicios eficientes que no discriminen y limiten directa o indirectamente a los usuarios por motivos técnicos o económicos.

- Educación digital. Las autoridades educativas deberán implementar políticas públicas inclusivas encaminadas a la promoción, fomento y difusión de una cultura de protección de datos personales, ante el uso de medios digitales en el sector educativo.

- Protección de datos personales de menores en internet. Las

instituciones educativas públicas y privadas en coordinación con los padres de familia, tutores o representantes legales de los menores que navegan en internet, deberán implementar mecanismos para garantizar la privacidad de los menores de edad en la red, a través de la supervisión de los niños y adolescentes mientras desarrollan sus actividades en el mundo digital, atendiendo al interés superior del menor y lo previsto en la normatividad aplicable en materia de protección de datos personales.

- Derechos ARCO en el entorno digital. Los prestadores de servicios de internet y los agentes de la sociedad de la información deberán implementar mecanismos y procedimientos para el ejercicio de los derechos ARCO en el entorno digital, atendiendo a los requisitos, plazos y procedimientos previstos en la normatividad aplicable en materia de protección de datos personales.

- Actualización de información en medios de comunicación digitales. Los medios de comunicación digitales deberán garantizar a los titulares, la inclusión de un aviso de actualización visible junto a las noticias, cuando la noticia original no refleje su situación actual ante actuaciones judiciales y ante posteriores determinaciones le genere un perjuicio.

- Derecho a la intimidad ante el uso de dispositivos digitales, videovigilancia, grabación de sonidos, geolocalización y desconexión digital en el ámbito laboral. En las relaciones laborales se debe implementar una expectativa razonable de privacidad.

- Derecho al olvido. Las personas tienen derecho a que se elimine de la lista de resultados de los motores de búsqueda, enlaces publicados que se obtengan a partir de la inclusión de su nombre; así mismo, tienen derecho a que se supriman sus datos personales otorgados para la publicación por servicios de redes sociales y servicios de la sociedad de la información, cuando la información sea inadecuada, excesiva e inexacta, atendiendo a los fines para los que fueron recabados, el plazo de conservación y el interés público de la información.

- Portabilidad. Los titulares tienen derecho a recibir una copia de los datos personales que hubieren facilitado a los responsables del tratamiento, o bien, a que se transmitan los datos personales entre los responsables, siempre que se cumplan las condiciones técnicas para su ejercicio.

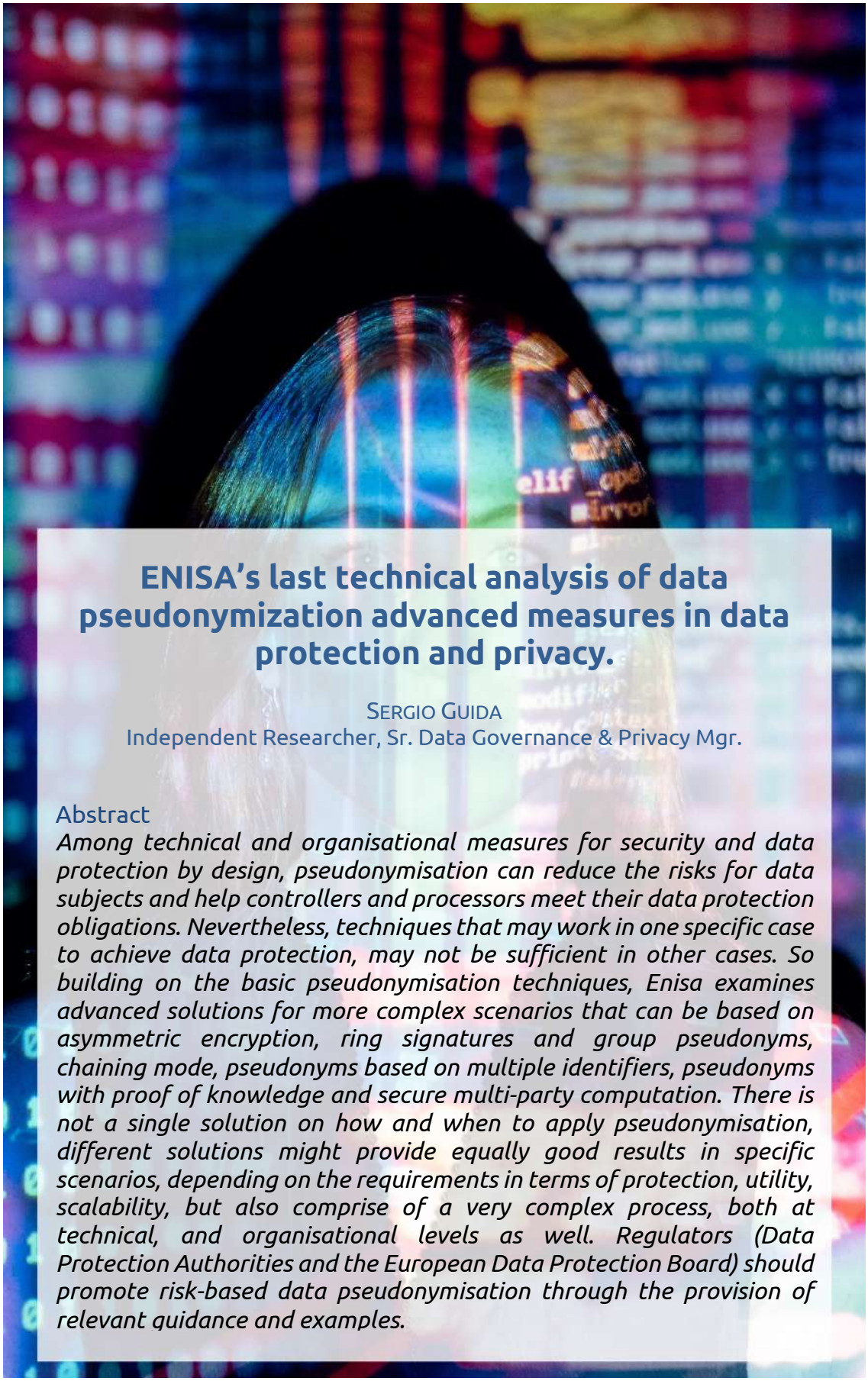
- Herencia digital. Los usuarios de los servicios de la sociedad de la información podrán determinar el destino, utilización o supresión del contenido generado en el entorno digital después de su fallecimiento.

Lo anterior, se manifiesta de manera enunciativa más no limitativa, ya que cada derecho digital tiene características específicas que requieren un análisis más detallado, a fin de incluir todos los aspectos relevantes en cada caso concreto que fortalezca el marco jurídico en materia de protección de datos

personales y posicionar a México como una nación que reconoce y garantiza el pleno ejercicio de los derechos digitales.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012



ENISA's last technical analysis of data pseudonymization advanced measures in data protection and privacy.

SERGIO GUIDA
Independent Researcher, Sr. Data Governance & Privacy Mgr.

Abstract

Among technical and organisational measures for security and data protection by design, pseudonymisation can reduce the risks for data subjects and help controllers and processors meet their data protection obligations. Nevertheless, techniques that may work in one specific case to achieve data protection, may not be sufficient in other cases. So building on the basic pseudonymisation techniques, Enisa examines advanced solutions for more complex scenarios that can be based on asymmetric encryption, ring signatures and group pseudonyms, chaining mode, pseudonyms based on multiple identifiers, pseudonyms with proof of knowledge and secure multi-party computation. There is not a single solution on how and when to apply pseudonymisation, different solutions might provide equally good results in specific scenarios, depending on the requirements in terms of protection, utility, scalability, but also comprise of a very complex process, both at technical, and organisational levels as well. Regulators (Data Protection Authorities and the European Data Protection Board) should promote risk-based data pseudonymisation through the provision of relevant guidance and examples.

Keywords: Data protection and security by design; pseudonymization; advanced cryptography.

Summary: Introduction. – 1. Advanced pseudonymisation techniques and some relevant operating aspects. – 1.1 Asymmetric encryption. – 1.2 Ring signatures and group pseudonyms. – 1.3 Chaining mode. – 1.4 Pseudonyms based on multiple identifiers or attributes. – 1.5 Pseudonyms with proof of ownership. – 1.6 Secure multiparty computations. – 1.7 Secret sharing schemes. – 2. Conclusions and recommendations for all relevant stakeholders. – 2.1 Defining the best possible technique. – 2.2. Advanced techniques for advanced scenarios. – 2.3 Establishing the state-of-the-art. – 2.4 Towards the broader adoption of data pseudonymization.

Introduction.

Pseudonymisation is becoming a key security technique and a way to implement data minimisation in various contexts, providing a means that can facilitate personal data processing, while offering strong safeguards for personal data protection. Complementing its past work[1], in this report ENISA analyses advanced pseudonymisation techniques and specific use cases that can help towards the definition of the state-of-the-art in this field.

1. Advanced pseudonymisation techniques and some relevant operating aspects.

Among advanced pseudonymisation[2] techniques, based on cryptographic techniques[3], the following are disclosed:

---

[1] *The first relevant report in January 2019 ("ENISA, 2019 – 1") presented an overview of the notion and main techniques of pseudonymisation in correlation with its new role under the GDPR. A second ENISA report followed in November 2019 ("ENISA, 2019 – 2") with a detailed analysis of the technical methods and specific examples and best practices for particular data sets (email addresses, IP addresses and more complex data sets).*

[2] *Cf. "Pseudonymisation is defined in article 4(5) of the GDPR as: 'the processing of personal data in such a manner that the personal data 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'. In GDPR, the data controller is the entity responsible to decide whether and how pseudonymisation will be implemented. Data processors, acting under the instructions of controllers, may also have an important role in implementing pseudonymisation. Recital (29) GDPR states that the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help data controllers and processors to meet their data protection obligations. Moreover, recital (30) states that measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller, when that controller has taken appropriate technical and organisational measures and that additional information for attributing the personal data to a specific data subject is kept separately", as we can read in ENISA, Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation. November 2018 in https://www.aepd.es/sites/default/files/2019-09/recomendations-on-shaping-technology-according-to-GDPR-provisions -1.pdf.*

[3] *Cryptographic techniques, such as encipherment, digital signatures, key management and secret sharing schemes, are important building blocks in the implementation of all security services. "You can define encryption as a means by which to convert readable content (plaintext) into unreadable gibberish (ciphertext). Encryption is a mathematical operation that exists within the realm of cryptography. However, there's an important difference:*

1.1 Asymmetric encryption.

Although symmetric encryption is most commonly used, asymmetric encryption has some interesting properties that could support data minimization, too, and the 'need-to-know principle'[4], while providing robust protection. There are two different entities involved during the pseudonymisation process:

(i) a first entity creates the pseudonyms from the identifiers using the Public pseudonymisation Key (PK), and

(ii) another entity is able to resolve the pseudonyms to the identifiers using the Secret (private) pseudonymisation Key (SK)[5].

They do not have to share the same knowledge: a data controller can make available its PK to its data processors, who can collect and pseudonymise the personal data using the PK, so the former is the only entity which can later compute the initial data from the pseudonyms. Such a scenario is related to the generic one of a data processor being the Pseudonymisation Entity, with the additional advantage, in terms of protecting individuals' identities, that the processors do not have the pseudonymisation secret. But, since the encryption key PK is publicly available, an adversary knowing both PK and the set of

---

- *Cryptography is the overarching term for the field of cryptographic communications.*
- *Encryption, on the other hand, refers to the actual process of encrypting plaintext data into unreadable ciphertext.*

Basically, encryption is the process of transforming plaintext into ciphertext through the use of two important elements:

- *Algorithms — An encryption algorithm is a set of directions to help you solve a problem. More specifically, it's a set of mathematical instructions and processes that serve a specific purpose. Some algorithms are designed to work in either private or public channels. So, you can have asymmetric or symmetric encryption algorithms. In general, encryption algorithms are useful for encrypting data. When coupled with authentication measures, they also protect data integrity.*
- *Keys — A cryptographic key is a long, random and unpredictable string of letters and numbers that you use to encrypt or decrypt data. No matter whether you're talking about asymmetric vs symmetric encryption, the keys are important to protect",*

as we can read in Casey Crane, Asymmetric vs Symmetric Encryption: Definitions & Differences, December 7, 2020 in https://www.thesslstore.com/blog/asymmetric-vs-symmetric-encryption/.

[4] *Cf. "This principle states that a user shall only have access to the information that their job function requires, regardless of their security clearance level or other approvals. In other words: a User needs permissions and a Need-to-know. And that Need-to-know is strictly bound to a real requirement for the User to fulfill its current role. As you might be able to tell by the choice of words the Need-to-know principle is typically enforced in military or governmental environments. Sometimes, in non-military scenarios, you will also find a slightly different description which states in weaker terms that access to data must be regularly reviewed to ensure that users only access data they strictly need for legitimate reasons. This is enforcement by regulation or rule rather than permissions and can be sufficient in the private sector. In information technology the Need-to-know can be implemented by using mandatory access control (MAC) as well as discretionary access control (DAC) in conjunction with a secondary control system" in https://techcommunity.microsoft.com/t5/azure-sql/security-the-need-to-know-principle/ba-p/2112393.*

[5] *Cf. "In asymmetric or public-key cryptography, two different keys are used, the first key (the public key) is used by the sender to encrypt the information, the second key is a private and secret key used by the recipient to decrypt the information. Therefore, the encryption key can be made public, a common secret is not needed to be agreed on by the parties in advance as the second secret key is only known by the recipient... This technique is used mostly for end-to-end encryption. Thus, in an asymmetric encryption scenario the private key has to be kept secret. The risk that a third party could obtain the key consequently arises e.g. if the secret key is stored at a cloud provider which also holds the public key or by man-in-the-middle attacks, if a third party misleads the other parties by pretending to be the respective counterpart. If all necessary security measures are complied with – in the sense of the relative approach – it is not reasonably likely that a man-in-the-middle attack occurs" in Gerald Spindler, Philipp Schmechel, Personal Data and Encryption in the European General Data Protection Regulation, 7 (2016) JIPITEC 163 par.1, in https://www.jipitec.eu/issues/jipitec-7-2-2016/4440.*

original identifiers can perform an exhaustive search attack for those schemes. Therefore it is important to use a randomised encryption scheme – i.e. at each encryption, a random value (nonce) is being introduced to ensure that for given input (user's identifier) and PK, the output (pseudonym) cannot be predicted, i.e. a different pseudonym is derived each time for the same identifier, without changing the process or the pseudonymisation secret[6].

Many asymmetric encryption schemes support homomorphic encryption[7], which is a specific type of encryption, allowing a third party (e.g. a cloud service provider) to perform certain computations on the ciphertexts without having knowledge of the relevant decryption key: e.g. the product of two pseudonyms created using Paillier's scheme[8] is the pseudonym of sum of the two identifiers. The generation speed and the size of the pseudonym obtained using asymmetric encryption can also be an issue, these parameters being strongly correlated to the size of the keys: for instance, in certain setups, the key size can be up to 2018 or 3096 bits.

A typical application is to make available healthcare data to research groups. In order to ensure that the identifiers (e.g. social security number or medical registration number) of a given patient are not linkable, a participant may have different local pseudonyms at doctors X, Y, Z, and at medical research groups U, V, W – thus providing domain-specific pseudonyms to ensure unlinkability between these different domains; so doctors will store both the real name/identity of their patients and their local pseudonyms, but researchers will only have (their own) local pseudonyms. As characteristic examples, ElGamal cryptosystem[9] has been used.

---

[6] *See Section 5.2.3 "ENISA, 2019 – 2".*

[7] *Cf. "Homomorphic encryption makes it possible to analyze or manipulate encrypted data without revealing the data to anyone. Just like other forms of encryption, homomorphic encryption uses a public key to encrypt the data. Unlike other forms of encryption, it uses an algebraic system to allow functions to be performed on the data while it's still encrypted. Then, only the individual with the matching private key can access the unencrypted data after the functions and manipulation are complete. This allows the data to be and remain secure and private even when someone is using it. Dr. Craig Gentry describes homomorphic encryption as a glovebox where anybody can get their hands into the glovebox and manipulate what's inside, but they are prevented from extracting anything from the glovebox. They can only take the raw materials and create something inside the box. When they finish, the person who has the key can remove the materials (processed data)" in Bernard Marr, What Is Homomorphic Encryption? And Why Is It So Transformative?, Forbes, Nov 15, 2019 in https://www.forbes.com/sites/bernardmarr/2019/11/15/what-is-homomorphic-encryption-and-why-is-it-so-transformative/.*

[8] *"From a conceptual viewpoint, encryption with the Paillier scheme consists of a fixed basis modular exponentiation with the message as exponent, and the generation of a noise factor used to mask the message. For fixed basis exponentiation, it is well-known that the performance can be increased by pre-computing powers of the fixed basis. By fine-tuning this and other known methods, we reduce the complexity of this step considerably. For the generation of the noise factor, we apply a new method that consists of using pre-computed noise to generate new noise factors. This reduces the bottleneck of noise computation to a few modular multiplications. Together, these methods achieve the considerable increase in encryption performance mentioned above" in Christine Jost, Ha Lam, Alexander Maximov, Ben Smeets, Encryption Performance Improvements of the Paillier Cryptosystem 2015 in https:// eprint.iacr.org/2015/864.pdf , page 2.*

[9] *"ElGamal is a public key system which uses modular exponentiation as the basis for a oneway trap door function. The reverse operation, the discrete logarithm, is considered intractable. ElGamal was never patented, making it an attractive alternative to the more well-known RSA system. Public key systems are fundamentally different from symmetric systems, and typically demand much larger keys. 1024 bits is the minimum recommended size for ElGamal, and even larger keys are recommended for some applications" in Bryce D. Allen, Implementing several attacks on plain ElGamal encryption, https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=2577&context=etd , page 7.*

1.2 Ring signatures and group pseudonyms.

Digital signatures constitute a main cryptographic primitive [10] towards ensuring both the integrity of the data as well as the authentication of the originating user, (the signer of the message), so that anybody can verify the validity of the signature associated with a known signer. Several advanced digital signature techniques are known, each aiming to fulfill the requirements of a specific application. The so-called 'ring signature' is based on asymmetric cryptography, as it is assumed that each possible signer (i.e. the k-th amongst n users, $1 \leq k \leq n$) is associated with a public key Pk and a relevant secret (private) key Sk. Any user from the group can generate, for any given message m, a signature s by appropriately using his/her secret key and the public keys of all the other members of the group. A verifier with access to the public keys of all members of the group is able to confirm that a given signed message m has been signed by a member of the group, but not to identify which user is the actual signer: for instance, a ring signature could be used to provide a verifiable signature from "a high-ranking official", without revealing who exactly is that official. Actually, it's a pseudonymous scheme, allowing for a specific utilisation (i.e. verifying that the data stem from a well-determined group of users), in which the pseudonymisation secret (i.e. the secret key) is under the sole control of the data subject.

Group pseudonyms have been used in many contact tracing protocols (like Pronto-C2[11]) proposed during the COVID-19 pandemic[12]: each time two data subjects meet, a pseudonym is created with a contribution from each data subject, so they both have computed the same pseudonym. Each data subject has a list of groups or encountered pseudonyms and, if one of them is exposed, all his/her group pseudonyms are published on a public board and all the contacts can check if they have been exposed. This pseudonymisation scheme has to be randomized, so that when two data subjects meet again, they get a

---

[10] *"Cryptographic primitives are well-established, low-level cryptographic algorithms that are frequently used to build cryptographic protocols for computer security systems. These routines include but are not limited to, one-way hash functions and encryption functions" in https://medium.com/geekoffee/ensuring-integrity-authenticity-and-non-repudiation-in-data-transmission-using-node-js-af73c2404153.*

[11] *Cf. Gennaro Avitabile, Vincenzo Botta, Vincenzo Iovino, Ivan Visconti, Towards Defeating Mass Surveillance and SARS-CoV-2: The Pronto-C2 Fully Decentralized Automatic Contact Tracing System. IACR Cryptol. ePrint Arch. 2020: 493 (2020) in https://eprint.iacr.org/2020/493.pdf :"In the 70s Merkle, Diffie and Hellman invented public-key cryptography. Starting with Merkle's puzzles, Diffie and Hellman proposed a key exchange protocol [DH76] (i.e., the Diffie-Hellman protocol) where two parties can establish a secret key K by just sending one message each on a public channel. A message consists of a group element in a setting where the so-called Decision Diffie-Hellman assumption holds. In our view, the most natural way to realize a privacy-preserving ACT system consists of having as pseudonym a group element that corresponds to a message in the DH protocol. This natural idea was also proposed to the DP-3T team. In order to actually realize such form of ACT system, one needs to solve the following two main problems. Anonymous call: realizing a mechanism that allows an infected party to use K in order to call the other party in a secure and privacy-preserving way. Shortening pseudonyms: making sure that the size of a group element fits the number of available bits in a BLE identifier beacon", page 7. "Notice that the approach of Pronto-C2 is therefore completely different from the one adopted in the DP-3T systems. Indeed, while in the DP-3T systems the pseudonyms of the infected person are broadcast to everyone (or added to a Cuckoo filter by the server that then transmits the filter) we instead ask the infected party to send a message that is understandable uniquely by the party with which she was in close proximity", page 8.*

[12] *For an in-depth discussion, see Sergio Guida, Un Framework per il Contact Tracing in Italia tra esigenze scientifiche, possibilità tecnologiche e rispetto di Diritti e Libertà Individuali in termini di Data Protection, European Journal of Privacy Law & Technologies, September 16, 2020 in http://www.ejplt.tatodpr.eu/Tool/Evidenza/ Single/view_html?id_evidenza=62.*

new group pseudonym to avoid any malicious traceability.

1.3 Chaining mode.

Not very often a secure cryptographic hash function[13] is expected to be an appropriate pseudonymisation technique, while authentication codes and keyed-hash functions are being preferred – which include the use of a secret key. However, more advanced techniques can be obtained by appropriately chaining hash functions, a layered approach in which several somehow intermediate pseudonyms are temporarily generated, in order to finally obtain the pseudonym, which is the output of the last hash function. Each layer is computed by a different entity who holds a secret used to obtain an intermediate pseudonym: K1 is used to obtain the temporary value X=$HK1(ID)$. Value X is then transmitted to the second entity which computes Y=$HK2(X)$. Finally, the last entity computes the $Pseudo$=$HK3(Y)$. Such a chain mitigates the risk of a data breach. An adversary needs to compromise the three entities in order to reverse the pseudonymisation, i.e. he/she must know K1, K2, K3.

Apparently, pseudonym resolution requires to have the three entities to cooperate and just that ensures an additional property that cannot be achieved by a single keyed hash function: any entity receiving an intermediate pseudonym cannot reverse it, whereas the first entity (which knows the original identifiers) is not able to match the final pseudonyms with the identifiers. For example, the recipient of the final pseudonym may perform statistical/scientific analysis on the pseudonymous data without being able to map the pseudonyms to the original users' identifiers. A hash chain can be further generalised into more articulated structures where, depending on the application scenario, each entity can apply a different pseudonymisation technique in this chaining approach.

1.4 Pseudonyms based on multiple identifiers or attributes.

Pseudonymisation is the processing of an identifier into a pseudonym, i.e. a one-to-one mapping, but to add new properties it can be the processing of several identifiers, many-to-one mapping.

The identifiers can be

- Homogeneous: they have the same type (only phone number for instance) and they are related to different individuals or

---

[13] *"A cryptographic hash function is an algorithm that takes an arbitrary amount of data input—a credential—and produces a fixed-size output of enciphered text called a hash value, or just "hash." That enciphered text can then be stored instead of the password itself, and later used to verify the user. Certain properties of cryptographic hash functions impact the security of password storage:*

- *Non-reversibility, or one-way function. A good hash should make it very hard to reconstruct the original password from the output or hash.*
- *Diffusion, or avalanche effect. A change in just one bit of the original password should result in change to half the bits of its hash. In other words, when a password is changed slightly, the output of enciphered text should change significantly and unpredictably.*
- *Determinism. A given password must always generate the same hash value or enciphered text.*
- *Collision resistance. It should be hard to find two different passwords that hash to the same enciphered text.*
- *Non-predictable. The hash value should not be predictable from the password,*

as we can read in https://www.synopsys.com/blogs/software-security/cryptographic-hash-functions/.

- Heterogeneous: they match different attributes of a single individual (social security number, phone number, first name and last name).

Any known pseudonymisation technique can be easily applied to more than one identifier, e.g. a keyed hash function, as pseudonymisation primitive, may have, as input data, a combination of more than one identifiers of an individual in order to derive a pseudonym for him/her (cf. "ENISA, 2019 – 1"). Now to ensure some additional properties of such pseudonyms which correspond to many-to-one-mappings, more sophisticated approaches are needed: cryptographic accumulators [14] are best fitted to implement a many-to-one pseudonymisation scheme. A cryptographic accumulator can accumulate a set L of values into a unique, small value z in such a way that it is possible only for elements y L to provide a proof that a given y actually has been accumulated within z. Such a proof is called a witness w.

Here follows an example based on Merkle Tree[15], a binary tree constructed through hash functions (which could be seen as a generalisation of hash chains). This structure properly suits the purposes of pseudonymization: a) the root of the tree is the pseudonym; b) the leaves of the tree correspond to the authentication codes of the identifiers computed using a message authentication code G and different keys. The inner nodes of the tree are computed using a cryptographic hash function H. The role of the authentication codes is to ensure that no dictionary attack is possible. The root and the inner nodes of the tree are computed using H to let anybody verify that a leaf is associated to a given root z (i.e. being the witness wi for the corresponding IDi). Generally, each contributor knows IDi and the corresponding witness wi (including the corresponding key ki) A contributor can later reveal IDi and wi to prove he/she has contributed to z. Actually, this property of Merkle trees is widely used in constructing one-time signature schemes that achieve post-quantum security.

It is impossible to revert the tree, i.e. recover any values ID1, ID2, ID3 or ID4 while knowing only its root (i.e. the accumulated pseudonym). If a subset of identifiers, ID1 and ID3 for instance, has been revealed, it is still not possible to

---

[14] *Cf. "A cryptographic accumulator is a short binding commitment to a set of elements and allows for, short membership proofs for any element in the set and/or, non-membership proofs for elements not inside the set. These proofs, also called witnesses (witness to element being accumulated in the accumulator), can be verified against the commitment. They are often used as communication-efficient authenticated data structure for remote databases, where individual elements with their proofs can be retrieved and efficiently verify integrity of the database. Accumulators can be categorized into Static and Dynamic. Unlike static variants, dynamic accumulators allow for addition/deletion of elements at cost independent of the size of the accumulated set. A dynamic accumulator is universal, if it supports both membership and non-membership proofs" in Amit Panghal, Cryptographic Accumulators: Part1, Medium, May 6, 2019 in https://medium.com/@panghalamit/cryptographic-accumulators-part1-3f23172d3fec.*

[15] *Cf. "A Merkle tree is a data structure that is used in computer science applications. In bitcoin and other cryptocurrencies, Merkle trees serve to encode blockchain data more efficiently and securely. They are also referred to as 'binary hash trees'. Breaking Down Merkle Tree: in bitcoin's blockchain, a block of transactions is run through an algorithm to generate a hash, which is a string of numbers and letters that can be used to verify that a given set of data is the same as the original set of transactions, but not to obtain the original set of transactions. Bitcoin's software does not run the entire block of transaction data – representing 10 minutes' worth of transactions on average – through the hash function at one time, however. Rather each transaction is hashed, then each pair of transactions is concatenated and hashed together, and so on until there is one hash for the entire block. (If there is an odd number of transactions, one transaction is doubled and its hash is concatenated with itself). Visualized, this structure resembles a tree" in Jake Frankenfield, Merkle Tree, Investopedia, Feb 18, 2020 in https://www.investopedia.com/terms/m/merkle-tree.asp.*

recover the other identifiers ID2 and ID4. It is only possible to know that ID2 and ID4 have accumulated into z if and only if their corresponding witnesses w2 and w4 have been revealed.

Similar structures can be generalized as any tree-structure starting with several types of personal data as its leaves and appropriately moving upwards via employing hashing operations preserves somehow the same properties as described above. The value at each internal node can be seen as an intermediate pseudonym, depending on one or more individual's attributes. The value z' of each intermediate pseudonym does not allow computation of the original personal data (i.e. pseudonymisation reversal), but allows for verification whether, for a given initial set of values, these values have accumulated into the pseudonym z' or not. Each intermediate pseudonym may be handled by a different entity.

1.5 Pseudonyms with proof of ownership.

In special cases, pseudonymisation may interfere with the exercise of the rights that a data subject has on his/her data as defined in the GDPR (Articles 15 to 20): for example, in cases where the data controller does not have access to original identifiers but only to pseudonyms [16], then any request from a data subject to the data controller can be satisfied only if the data subject is able to prove that the pseudonym is related to his/her own identity.

Although the pseudonym is a type of an identifier, if its association with a specific data subject cannot be appropriately established, to avoid that the data controller cannot satisfy relevant requests, 'pseudonyms with proof of ownership' are required: a pseudonym P is created by a data subject from a given identifier ID and later transferred to a data controller. The hiding property states that the data controller must not be able to recover any information from the pseudonym P: this property is important to avoid exposing the personal data of the data subject. At the same time, it must not be possible to find another identifier ID'≠ ID that is associated to P: this is the binding property. This property is needed to avoid any ambiguity on the identity of the data subject associated with a pseudonym, since otherwise it would be impossible to differ between two data subjects. It prevents impersonation attack when a right is exercised on the data. These two properties, hiding and binding, can be achieved by 'cryptographic commitment scheme'[17], having also considered that the identifier is a public key from an

---

[16] *This is a rather common situation in experimental clinical studies (RCT, 'randomized controlled trial', typically) that take place in various centers, often in different countries. It may happen that the patient resident in a State wants to request his/her data from the Study Coordinator at the 'Sponsor', which can be located in a different country: in such cases, the pseudonymisation techniques used by the data controller(s) must allow access to the data to take place with the appropriate guarantees but without any problem or delay for the data subject (patient).*

[17] *"The notion of commitment is at the heart of almost any construction of modern cryptographic protocols. In this context, making a commitment simply means that a player in a protocol is able to choose a value from some (finite) set and commit to his choice such that he can no longer change his mind. He does not however, have to reveal his choice - although he may choose to do so at some later time. There are many ways of realizing this basic functionality, some are based on physical processes, e.g. noisy channels or quantum mechanics, while others are based on distributing information between many players connected by a network. We will say a bit more about this later, but for now we will concentrate on the scenario that seems to be the most obvious one for computer communication: commitments that can be realized using digital communication between two players.*

asymmetric encryption scheme. When the data subject needs to exercise his/her rights (an access request), he/she needs to succeed a challenge/response protocol and to open the commitment; the data controller asks the subject to sign using its private key SKa, providing also all the values needed to let the data controller verify the pseudonym: it includes, apart from the signature R, the public key PKa and the value k.

To check if any request made by the data subject related to a specific pseudonym is legitimate or not, the data controller must ensure that PKa matches the pseudonym and that the signature is correct using PKa.

1.6 Secure multiparty computations.

A secure Multiparty Computation[18] (MPC) protocol allows a set of parties to jointly compute a function of their secret inputs without revealing anything but only the output of the function. Applications include privacy-preserving auctions and private comparisons of lists.

A specific case of secure MPC is the private set intersection protocol, in which two parties with private lists of values wish to find the intersection of the lists, without revealing anything apart from the elements in the intersection, by means of a 'oblivious Pseudorandom Function' [19] (PRF) F;

As a very simple example of this kind of commitments, consider the case where P has a pair of RSA keys, where V (like anyone else) knows the public key with modulus n and public exponent e. To commit to a bit b, P can build a number xb, which is randomly chosen modulo n, such that its least significant bit is b. Then he sends the encryption C = x e b mod n to V. We do not prove anything formal about this scheme here, although that is in fact possible. But it should be intuitively clear that P is stuck with his choice of b since the encryption C determines all of xb uniquely, and that V will have a hard time figuring out what b is, if he cannot break RSA. Thus, at least intuitively, the binding and hiding requirements are satisfied" in Damgård, Ivan & Nielsen, Jesper, Commitment Schemes and Zero-Knowledge Protocols (2007). Lecture Notes in Computer Science – LNCS in https://www.researchgate.net/publication/245702839_Commitment_Schemes_and_Zero-Knowledge_Protocols_2007, pages 1-2.

[18] Cf. "Secure multi-party computation (MPC) enable a group to jointly perform a computation without disclosing any participant's private inputs. The participants agree on a function to compute, and then can use an MPC protocol to jointly compute the output of that function on their secret inputs without revealing them. Since its introduction by Andrew Yao in the 1980s, multi-party computation has developed from a theoretical curiosity to an important tool for building large-scale privacy-preserving applications" (page 5). "The term secure computation is used to broadly encompass all methods for performing computation on data while keeping that data secret. A computation method may also allow participants to confirm the result is indeed the output of the function on the provided inputs, which is known as verifiable computation" (ibidem). "The goal of secure multi-party computation (MPC) is to enable a group of independent data owners who do not trust each other or any common third party to jointly compute a function that depends on all of their private inputs. MPC differs from outsourced computation in that all of the protocol participants are data owners who participate in executing a protocol" (page 8) in David Evans, Vladimir Kolesnikov and Mike Rosulek, A Pragmatic Introduction to Secure MultiParty Computation. NOW Publishers, 2018. (This version: April 15, 2020) available at https://www.cs.virginia.edu/~evans/pragmaticmpc/pragmaticmpc.pdf.

[19] "Before defining pseudorandom function, we first recall the definition of a random function. We can describe a random functions in two different ways: a combinatorial description—as a random function table—and compuational description—as a machine that randomly chooses outputs given inputs and keeps track of its previous answers. In the combinatorial description, the random function table can be view as a long array that stores the values of f. So, f(x) returns the value at position nx. The problem with random functions is that (by definition) they have a long description length. So, we cannot employ a random function in our encryption scheme. We will next define a pseudorandom function, which mimics a random function, but has a short description. Intuitively, a pseudorandom function (PRF) "looks" like a random function to any n.u. p.p.t. adversary. In defining this notion, we consider an adversary that gets oracle access to either the PRF, or a truly random function, and is supposed to decide which one it is interacting with. More precisely, an oracle Turing machine M is a Turing machine that has been augmented with a component called an oracle: the oracle receives requests from M on a special tape and writes its responses to a tape in M. We now extend the notion of indistinguishability

namely, this is a two-party protocol between a sender S and a receiver R so as, for a secret key k provided by S (and being hidden from R) and for any input v from R, R computes the value Fk(v) (without learning the key k) and S does not learn the input v. So, if the private lists consist of personal data, a secure MPC protocol actually provides the means for sophisticated pseudonymisation schemes: assuming that xi, yj are e-mail addresses of users, 1 ≤ i, j ≤ n, the outputs of the PRF function Fk(xi) and Fk(yj) are actually pseudonyms, where the key k is the pseudonymisation secret. Such techniques for private set intersection may be the proper solutions in terms of personal data protection in situations where comparison of two different lists from two different data controllers are required without revealing anything else than their common entries, such as, for example, if two health insurance companies wish to ensure that no one has taken out the same insurance with both of them. It is used also for advertising purposes, i.e. measuring adv conversion rates by comparing the list of people who have seen an ad with those who have completed a transaction, where these lists are held by the advertiser and by merchants, respectively.

1.7 Secret sharing schemes.

Secret sharing schemes can be seen as specific instances of secure Multiparty Computation (MPC) protocols. They are well known cryptographic techniques, aiming to appropriately split a secret information D into n parts D1, D2, . . ., Dn so as to ensure the following:

- Knowledge of k (or more) of D1, D2, . . ., Dn allow to compute D (where k is a design parameter)
- Knowledge of k – 1 (or fewer) of D1, D2, . . ., Dn is not sufficient for the computation of D.

Such schemes are also known as (k, n) threshold schemes and this is an approach to securely manage a secret cryptographic key: if on the one hand, storing the key in a single, well-guarded location is unreliable in terms of single misfortune or corruption, on the other hand storing multiple copies of the key at different locations increases the risk of security breaches. Instead, by using a (k, n) threshold scheme with n = 2k - 1, a robust key management scheme is available: we can recover the original key even if almost the half (k -1) of the n pieces are destroyed, whilst at the same time an adversary cannot reconstruct the key even if any k -1 such segments are compromised. As Adi Shamir stated, “threshold schemes are ideally suited to applications in which a group of mutually suspicious individuals with conflicting interests must cooperate (...) By properly choosing the k and n parameters we can give any sufficiently large majority the authority to take some action while giving any sufficiently large minority the power to block it”.

Such a technique can be used to split an identifier into distinct pseudonyms:

of distributions, to indistinguishability of distributions of oracles. The intuition about why f is a pseudorandom function is that a tree of height n contains 2n leaves, so exponentially many values can be indexed by a single function with n bits of input. Thus, each unique input to f takes a unique path through the tree. The output of f is the output of a pseudorandom generator on a random string, so it is also pseudo-random” in Raphael Pass, Abhi Shelat, A Course in Cryptography, 2010, pages 94 - 97 in https://www.cs.cornell.edu/ courses/cs4830/2010 fa/lecnotes.pdf.

let us assume that the Pseudonymisation Entity substitutes (through a mapping procedure) the user's identifier by carefully chosen pseudonyms. Each of these pseudonyms is irreversible (i.e. its recipient cannot compute the original identifier), under the assumption that the pseudonymisation mapping remains secret. Moreover, the unlinkability property is ensured since all these pseudonyms are different.

In case of need, these pseudonyms can be used for re-identification, too, but only if a well-determined number of the recipients agree to exchange their different pseudonym for the same entity pseudonyms. For example, this approach could be used to pseudonymise auditing log files of a system so as to ensure that pseudonymisation reversal will occur only if a suspicious activity is present: then, the parties storing the pseudonyms (i.e. the log events analysers) are able to derive the original identifier by exchanging the corresponding values of the pseudonyms. Otherwise, no identification of users from their relevant log data is possible. Another secret sharing scheme has been used to protect vehicular identity privacy in a Vehicular Ad Hoc Network (VANET), constituting a main application field for the Internet-of-Things (IoT), which generally poses demanding challenges to the personal data protection.

Because of the inherent properties of secret sharing schemes, we can conclude that the pseudonymisation secret is somehow shared across multiple entities (this could be a case of joint controllership). In fact, in the above scenario, each pseudonym also plays, in a sense, the role of a part of the secret of the pseudonymization: indeed, in a (k, n) scheme, combination of any k such shares (but no less) suffices to extract the original identifier.

This idea of sharing the secret of pseudonymisation can also be applied in other pseudonymisation techniques, for example, assuming a technique where the pseudonymization secret itself is a secret key.

Since the secret of the pseudonymisation is inextricably linked to the additional information necessary to attribute the pseudonymous data to a specific data subject, and the GDPR establishes that, pursuant to Article 4 (5), such additional information must be kept separately and be subject to technical and organizational measures, it is clear that secret sharing schemes can provide the means to achieve these goals. Therefore, it is understood how complex the task of selecting the optimal parameters and settings for sharing secrets can become to securely store the secret data shares, while satisfying all the requirements of the end user and all the 'boundary conditions'.

2. Conclusions and recommendations for all relevant stakeholders.

2.1 Defining the best possible technique.

A risk-based approach[20] to pseudonymisation is fundamental to unfold the

[20] *Not only taking into account specifically the risks for rights and freedoms of natural persons, as required by the GDPR, but also in a broader sense: "A holistic approach proceeds from an accurate overview of the risk landscape—a governing principle that first of all requires accurate risk reporting. The goal is to empower organizations to focus their defenses on the most likely and most threatening cyber risk scenarios, achieving a balance between effective resilience and efficient operations. Tight controls are applied only to the most crucial assets. The holistic approach lays out a path to root-cause mitigation in four phases: 1. Identify risks and risk*

potentials of this set of technologies. There is no' fit-for-all' pseudonymisation technique and a detailed analysis of the case in question is necessary in order data controllers and processors to define the best possible option. For instance, although simple hash would not provide adequate data protection in most cases, appropriate elaboration of this technique (as in the case of chaining mode or Merkle trees) can significantly increase the protection level.

Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should promote risk-based data pseudonymisation by providing relevant guidance and examples.

2.2. Advanced techniques for advanced scenarios.

Technical solutions are of course a critical element for achieving correct pseudonymisation, but the organizational model and underlying structural architecture are 'critical success factors' (CSF) as well. In practice, before implementing a solid pseudonymisation technique, you need to make sure that the entities involved (and the associated data flow scheme) will be able to support it. Data controllers and processors should always imagine scenarios capable of supporting advanced pseudonymisation techniques, based, inter alia, on the principle of data minimization.

The research community should indicate to data controllers and processors the elements of trust and the necessary guarantees so that the advanced scenarios are then functional in practice.

Finally, regulators should ensure that regulatory approaches, e.g. relating to new technologies and application sectors, consider all possible subjects and roles from the data protection point of view, while remaining technologically neutral.

2.3 Establishing the state-of-the-art.

Much remains to be done to define the state of the art, for example, to work on more complex cases and their possible future evolution in the light of emerging technologies. To this end, research and application scenarios need to go hand in hand, involving all stakeholders (researchers, industry and regulators) to discuss joint approaches.

The European Commission, relevant EU institutions, as well as Regulators should support the creation and maintenance of the state of the art in pseudonymisation, bringing together fields (regulators, research community and industry).

The research community should continue its efforts to advance existing work on data pseudonymization, addressing the special challenges that arise

---

appetite. 2. Analysis and evaluation. 3.Treatment. 4.Monitoring… Among the most important instruments for fostering discipline throughout the organization are scheduled status updates to senior management on top cyber risks, treatment strategy, and remediation" in Jim Boehm, Peter Merrath, Thomas Poppensieker, Rolf Riemenschnitter, and Tobias Stähle, Cyber risk measurement and the holistic cybersecurity approach, McKinsey, November 2018 Risk Practice, in https://www.mckinsey.com/~/media/McKinsey/BusinessFunctions/Risk/OurInsights/Cyberriskmeasurementandtheholisticcybersecurityapproach/Cyber-risk-measurement-and-the-holistic-cybersecurity-approach-vf.pdf, pages 3 to 5.

from emerging technologies, such as AI.

2.4 Towards the broader adoption of data pseudonymization.

Advancements such as

- CJEU Schrems II Judgment[21]:"Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems - Judgment of the Court (Grand Chamber), 16 July 2020. The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield[22]";
- the increasing need for open data access;
- big data: "in the case of big data, it is difficult to guarantee the confidentiality of a person or a group of people when databases from different sources are combined, even when the data were entered in an encoded or anonymized form[23]"

are enlighting the need to further advance appropriate safeguards including supplementary measures for personal data protection, including broader adoption and real world usage of pseudonymisation in different application scenarios.

---

[21] Cf."In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary. On the basis of the findings made in that decision, the Court pointed out that, in respect of certain surveillance programmes, those provisions do not indicate any limitations on the power they confer to implement those programmes, or the existence of guarantees for potentially targeted non-US persons. The Court adds that, although those provisions lay down requirements with which the US authorities must comply when implementing the surveillance programmes in question, the provisions do not grant data subjects actionable rights before the courts against the US authorities", we can read in the 'RESUME'' at http://curia.europa.eu/juris/document/document_print.jsf?docid=228728.

[22] For detailed analysis and commentary, see Sergio Guida, Caso Schrems II: Corte di Giustizia dell'Unione europea invalida la Decisione della Commissione sull'adeguatezza della protezione fornita dallo 'scudo UE-USA per la privacy' (Privacy Shield), in Data Protection Law-Rivista di Diritto delle nuove tecnologie, privacy e protezione dati, July 27,/2020 in https://www.dataprotectionlaw.it/2020/07/27/caso-schrems-ii-corte-di-giustizia-dellunione-europea-invalida-la-decisione-della-commissione-sulladeguatezza-della-protezione-fornita-dallo-scudo-ue-usa-per-la-privacy-privacy/.

[23] Cf Pilar Sanz, Key Points for an Ethical Evaluation of Healthcare Big Data. Processes. 7. 493. (2019) in https://www.researchgate.net/publication/334852654Key_Points_for an_Ethical_Evaluation_of_Healthcare_Big_Data.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Il danno non patrimoniale per lesione del legame tra individuo e agente intelligente.

Non-pecuniary damages resulting from harm to relationship between a human being and an intelligent agent.

LUIGI FILIPPO NAPPI
Collaboratore della cattedra di Diritto delle nuove tecnologie,
Università degli Studi Suor Orsola Benincasa

Abstract

Il panorama delle relazioni che interessano la sfera dell'individuo umano andrà incontro nel prossimo futuro ad un arricchimento significativo, da imputarsi all'interazione con i nuovi device basati sull'Intelligenza Artificiale. L'indagine che segue intende verificare, in primo luogo, la reale possibilità di tale nuovo paradigma di relazione non interumana e, in secondo luogo, le prospettive di tutela giuridica, con specifico riguardo al profilo della responsabilità per danno non patrimoniale.

The landscape of relationships that affect the sphere of the human individual will meet in the near future to a significant enrichment, due to the interaction with new devices based on artificial intelligence. The following investigation aims to verify, first, the real possibility and the nature of this new paradigm of non-interhuman relationship and, secondly, the prospects of legal protection, with specific regard to the profile of liability for non-pecuniary damage.

Parole chiave: protezione dei dati; informativa privacy; consenso; trasparenza; GDPR; legal design.

Keywords: data protection; privacy notice; consent; transparency; GDPR; legal design.

Introduzione.

L'agente dotato di intelligenza artificiale è, secondo le definizioni più autorevoli, un "agente intelligente" in possesso di spiccate capacità di interazione con l'ambiente circostante[1]. Un'area rilevante della capacità di interazione dell'I.A. è senza dubbio quella relazionale, come testimoniato, peraltro, dal "Test di Turing"[2], e, soprattutto, dal dato inconfutabile del massiccio impiego odierno dell'I.A. proprio in questo ambito. Un primo riferimento può riguardare gli assistenti vocali "smart", che oggi, con lo sviluppo dell'IoT, sono integrati con tutti i dispositivi principali dell'ambiente domestico, determinando un importante passo in avanti anche nello sviluppo della cd. domotica[3]. Non solo: l'impiego dell'I.A. con funzione "relazionale" registra un recente sviluppo nel campo del *customer care* aziendale, con la diffusione di assistenti in *chat* di supporto intelligenti[4], e in chiave più futuristica nei *call center*. Ancora, non bisogna dimenticare lo sviluppo recente di robot in grado di assistere soggetti deboli o malati attraverso un vero e proprio supporto psicologico[5]. In ultimo, gli sviluppi a cui è andata incontro la tecnologia hanno portato alla realizzazione di dispositivi in grado di aumentare alcune facoltà proprie dell'individuo[6] come la memoria; e questo, si badi, in

[1] S. Russel, P. Norvig., *Artificial Intelligence, A Modern Approach*, Pearson Education, 2nd Edition, 2003.
[2] Il test, elaborato nel 1970, prevede il coinvolgimento di tre soggetti A, B, C. A è un umano separato da B e C in modo tale che né la voce né l'aspetto visivo di questi ultimi due sia dal primo intelligibile. B e C sono, nella prima fase dell'esperimento due esseri umani di sesso opposto. A deve indovinare il sesso di B e C basandosi esclusivamente su di una conversazione scritta in cui B cercherà di trarre in inganno A, mentre C di agevolare il suo compito. Nella seconda fase dell'esperimento a B viene sostituita una macchina che continua a dover svolgere lo stesso ruolo nel gioco. Se alla fine dell'esperimento definito emblematicamente "Imitation Game" la percentuale in cui A ha risposto correttamente al quesito non è variata tra la prima e la seconda fase, allora la macchina in questione, può considerarsi a pieno titolo un agente intelligente.
[3] Si pensi, a titolo esemplificativo all'assistente *Alexa* (https://it.wikipedia.org/wiki/Amazon_Alexa), della multinazionale Amazon o al corrispondente di Google, *Google Assistant* (https://it.wikipedia.org/wiki/Assistente_Google).
[4] I cd. *chat bot* sviluppati per agevolare la risoluzione di problemi ed utilizzati dalla maggior parte delle piattaforme che offrono servizi on-line (vedi ad esempio https://yellow.ai/?utm_source=Marketing&utm_medium=google-search&utm_campaign=ai-chatbot).
[5] A titolo esemplificativo: *Alfred: a virtual assistant helping older people stay active* (https://digital-strategy.ec.europa.eu/en/news/alfred-virtual-assistant-helping-older-people-stay-active#:~:text=The%20Alfred%20project%20created%20a,people%20can%20interact%20with%20online.&text=The%20EU%2Dfunded%20Alfred%20project,from%20carrying%20out%20everyday%20tasks).
[6] Il tema dello "human enanchement" è stato, peraltro, ampiamente trattato da illustri esponenti della dottrina tra cui U. Ruffolo, *Intelligenza artificiale - Il diritto, i diritti, l'etica*, Milano, 2020 e U. Ruffolo A. Amidei,

assenza di una vera e propria *user interface* ma, piuttosto, integrandosi direttamente con il cervello umano[7].

Lo sviluppo di questa capacità dell'I.A. porta ad interrogarsi sulla dimensione sociale che la interazione tra essere umano e agente intelligente potrà assumere in futuro[8], ed in particolare sulla configurabilità di un diritto alla relazione con il robot[9], eventualmente giustiziabile sotto il regime della responsabilità per danno non patrimoniale. In questo specifico paradigma, peraltro, le ipotesi concretamente prospettabili di danno-evento appaiono molteplici: dalla distruzione volontaria o accidentale ad opera di un terzo del robot con cui il proprietario aveva instaurato un rapporto d'affezione, alla inizializzazione (*reset*) del *software* (attribuibile al produttore, o ad un attacco hacker di terze parti) con conseguente perdita di tutto il patrimonio di "ricordi" condivisi con il robot e immagazzinati nella sua memoria.

In sintesi, i passaggi concettuali da compiere nella trattazione di questo lavoro corrispondono ai due interrogativi appena esposti:

- Se sia realmente possibile un rapporto affettivo tra uomo e robot, e, in caso affermativo quanto siffatto genere di legame si differenzi dal rapporto tra umani o da rapporti già socialmente riconosciuti come, a titolo esemplificativo, quello tra uomo e animale domestico.
- Se, avendo risposto affermativamente risposto al primo quesito, il sorgere di legami di natura affettiva tra uomo e robot possa effettivamente dar vita ad un interesse alla conservazione di tali legami meritevole di tutela.

1. I rilievi delle scienze sociali sulla natura della relazione con il robot.

Da una disamina dei contributi dei principali esperti in I.A. e scienze sociali emergono una serie di considerazioni comuni in merito al primo interrogativo posto. Anzitutto, la sempre maggiore vicinanza alla sfera privata individuale dei *device* intelligenti potrebbe costituire un indizio positivo in tal senso, stante la naturale propensione dell'uomo a sviluppare una sorta di attaccamento in base ad un vissuto emozionale "condiviso"[10]. Altra considerazione particolarmente pregnante riguarda il ruolo che i robot stanno assumendo gradualmente nella società odierna: essi sono impiegati nello svolgimento mansioni rischiose che

---

Intelligenza Artificiale e diritti della persona: le frontiere del "transumanesimo" in U. RUFFOLO, *(a cura di) Intelligenza artificiale e diritto*, in *Giur. it.*, 2019, VII, 1657 – 1778.

[7] https://www.inverse.com/article/30609-elon-musk-neuralink-aging.

[8] Questo interrogativo, si badi bene, riguarda un'ampia categoria di robot, tra questi ad esempio, il veicolo ad alta automazione. Infatti, seppure il ruolo essenziale svolto dall'I.A. sul veicolo ad alta automazione non sia finalizzato all'interazione con gli occupanti, ma con l'ambiente circostante, ai fini dello svolgimento della guida autonoma o semi autonoma, è molto probabile che le capacità relazionali dell'HAV con gli occupanti diventino in futuro un aspetto di pari rilievo. Basti ragionare sul fatto che alla relazione personale col proprio veicolo tradizionale alcuni attribuiscono già un valore affettivo e che dunque anche il grado di interazione con gli occupanti potrebbe diventare alla lunga un fattore di scelta per l'acquirente.

[9] Ai fini della trattazione si avverte che il termine robot sarà utilizzato con lo stesso significato attribuito al termine "agente intelligente". In verità, i due termini non sono perfettamente sostituibili in ogni contesto, ma nel caso di specie le differenze sono sostanzialmente trascurabili.

[10] Tema, peraltro, ampiamente trattato da illustri esponenti della dottrina tra cui RUFFOLO U., *Intelligenza artificiale - Il diritto, i diritti, l'etica*, Milano, 2020 e U. RUFFOLO, A. AMIDEI, *Intelligenza Artificiale e diritti della persona: le frontiere del "transumanesimo"* in U. RUFFOLO, *(a cura di) Intelligenza artificiale e diritto*, in *Giur. it.*, 2019, VII, 1657 – 1778.

un tempo erano necessariamente eseguite da animali o dagli stessi esseri umani. Un esempio è costituito dai robot che in contesti militari sono impiegati per disinnescare ordigni esplosivi. È stato osservato, in uno studio svolto sul campo, che in contesti del genere gli operatori "umani" sviluppano un sentimento simile alla gratitudine nei confronti del robot che opera in una situazione di alto rischio al loro posto e sotto la loro guida[11]. In questo caso è possibile riportare questa considerazione al caso del veicolo ad alta automazione[12]. Possiamo infatti immaginare l'instaurarsi di un forte legame tra veicolo autonomo e suo proprietario laddove, in un frangente di pericolo, il primo abbia messo in salvo il secondo attraverso una manovra d'emergenza. In questo caso, il rapporto tra i due potrebbe somigliare, ad esempio, al rapporto d'affezione tra padrone e animale domestico che nel corso della comune convivenza ha difeso il primo in una situazione di pericolo.

Le considerazioni esposte inducono tutte a ritenere plausibile la futura formazione di legami affettivi, ma di certo non fanno luce sulla natura specifica di questi legami. Nel tentativo di approfondire questo aspetto, le scienze cognitive[13] hanno tentato di individuare gli elementi comuni alle relazioni tra due partner umani e tra uomo e animale di compagnia (unici due paradigmi che godono di pacifica e generale accettazione), per verificare che questi siano astrattamente riscontrabili anche nella nuova categoria relazionale: il rapporto tra individuo umano e robot.

Il primo elemento individuato è denominato dalla dottrina "attaccamento"[14]. Il significato dell'attaccamento risente del tipo di relazione in cui è osservato[15], e perciò non risulta facilmente individuabile avulso da un particolare contesto. In generale, tuttavia, si può intendere quale legame di particolare intensità che unisce i due *partner*, rendendo la separazione, anche temporanea, fonte di malessere. L'attaccamento si verifica sia nel rapporto interumano, che in quello tra uomo e animale da compagnia, ma, soprattutto, è un elemento presente nei legami affettivi con oggetti della vita quotidiana[16]. Di qui la trasversalità dell'attaccamento, che parrebbe principalmente fondato sulla presenza di un patrimonio di vissuto emozionale in qualsiasi modo collegato al proprio *partner*.

---

[11] ttps://www.forbes.com/sites/patricklin/2016/02/01/relationships-with-robots-good-or-bad-for-humans/.

[12] Il veicolo ad alta automazione (o *Highly Automated Vehicle*, HAV) può essere definito come un veicolo dotato di tecnologie che permettono lo svolgimento autonomo o semi-autonomo delle operazioni essenziali per la sua circolazione su strada. Si tratta, in particolare, dello svolgimento dei comandi detti di guida orizzontale (essenzialmente, il controllo della traiettoria del veicolo) e verticale (controllo della velocità del veicolo).

[13] D. LEVY, Love + Sex with Robots: *The Evolution of Human-Robot Relationships*, Blackstone Pub, 2nd Edition, 2010

[14] Il termine inglese *attachment* non sembra trovare corrispondente migliore che quello letterale in questo caso.

[15] La primigenia forma di attaccamento è quella presente tra infante e madre, in seguito una forma di attaccamento si sviluppa in forma analoga tra l'infante e i suoi primi giocattoli, su cui egli esercita un certo grado di controllo. Questa forma di attaccamento determina una prima emancipazione dell'infante dalla relazione di dipendenza dalla madre (D.W. WINNICOTT (1953). *Transitional objects and transitional phenomena; a study of the first not-me possession* in *The International Journal of Psychoanalysis, 34,* 89–97). Infine, una ulteriore declinazione dell'attaccamento si riscontra nell'età adulta con il partner romantico (C. HAZAN, P. SHAVER (1987). *Romantic love conceptualized as an attachment process* in *Journal of Personality and Social Psychology, 52*(3), 511–524).

[16] D. LEVY, op. cit., 28. In particolare, è il prolungato possesso dell'oggetto materiale che genera il legame, laddove nelle relazioni interumane questo è consolidato dalla vicinanza col proprio partener.

Secondo requisito individuato dalla dottrina scientifica è la possibilità di antropomorfizzazione del partner. La teoria secondo la quale ciascuna relazione non interumana debba passare necessariamente per l'umanizzazione dell'ente *partner* non umano è stata confermata con riferimento al rapporto tra uomo e animale domestico da autorevoli studi: questi hanno dimostrato la naturale propensione del proprietario ad interpretare in chiave antropomorfizzante i comportamenti dell'animale da compagnia [17]. L'antropomorfizzazione è, peraltro, alla base del rapporto affettivo-romantico con gli oggetti materiali (diremmo: inanimati), dapprima categorizzato dalla dottrina prevalente come forma di parafilia (denominata "oggettofilia") e più di recente riconsiderato da alcuni studiosi come un vero e proprio orientamento romantico [18]. Il caso del binomio relazionale essere umano-oggetto è emblematico, in quanto testimonia una spinta verso un graduale "sdoganamento" delle relazioni con l'altro "non umano", proveniente proprio dal crescente interesse della psicologia verso nuovi paradigmi, resi a loro volta oggetto di studio nell'ambito della categoria di recente matrice delle relazioni "non normative" [19]. Con riguardo a questo specifico caso, l'antropomorfizzazione è stata in particolare ravvisata nel linguaggio adoperato dai soggetti coinvolti nelle interazioni con gli oggetti materiali.

Anche la tendenza ad antropomorfizzare agenti intelligenti, che potremmo considerare come oggetti in possesso di potenzialità di interazione sicuramente superiori, è già stata evidenziata dalla comunità scientifica[20], e ciò porta a immaginare che sotto questo profilo non vi siano ostacoli alla genesi di un legame affettivo con il robot.

2. I riflessi nell'ambito della dottrina giuridica e della giurisprudenza.

Il complessivo quadro dottrinale in ambito scientifico in materia sembra, a questo punto, far emergere indizi sostanziali che tendono verso la possibilità di un nuovo paradigma relazionale. Inoltre, come visto, importanti segnali nel senso di uno sdoganamento dei rapporti con soggetti "non umani" provengono anche dal contesto sociale. Questi segnali non sono stati trascurati dalla più attenta dottrina giuridica, la quale, con lodevole lungimiranza, ha già speso alcune considerazioni in relazione alla evoluzione degli istituti giuridici odierni alla luce della diffusione di robot capaci di stringere legami affettivi con l'individuo umano.[21] Sulla questione specificamente oggetto della trattazione

[17] M. FIDLER, P. LIGHT, & A. COSTALL (1996). *Describing dog behavior psychologically: Pet owners versus non-owners. Anthrozoös*, *9*(4), 196-200.
[18] H. MOTSCHENBACHER, *Language, normativity and power: The discursive construction of objectophilia*, 2014.
[19] Per una panoramica sulla letteratura rilevante: https://www.oxfordbibliographies.com/view/document/obo-9780199756384/obo-9780199756384-0238.xml.
[20] B. REEVES, & C. I. NASS, (1996). *The media equation: How people treat computers, television, and new media like real people and places.* Center for the Study of Language and Information; Cambridge University Press.
[21] Si veda su tutti L. GATT, che in anticipo rispetto agli altri esponenti della dottrina pone il problema della futura ammissibilità del matrimonio con il robot. (*Il diritto di famiglia nell'era digitale: "Matrimonio coi Robots"*, intervento in occasione della conferenza intitolata: *Il diritto di famiglia nell'era digitale*, tenutasi martedì 24 ottobre 2017, presso la Facoltà di Giurisprudenza dell'Università degli studi "Suor Orsola Benincasa" di Napoli).

di questo lavoro, ossia la tutela risarcitoria del soggetto che subisca la lesione del suo diritto alla sfera relazionale con il robot, bisogna spendere, tuttavia, più approfondite considerazioni nel merito.

Per iniziare ad inquadrare meglio il contesto è necessario accennare che la Suprema Corte ha di recente riaffermato il diritto all'intangibilità della sfera degli affetti reciproci [22] , con conseguente risarcibilità del danno non patrimoniale [23] sofferto a seguito della morte di un congiunto, anche in relazione a soggetti non conviventi. In tale occasione la stessa ha affermato che:

«In caso di perdita definitiva del rapporto matrimoniale e parentale, ognuno dei familiari superstiti ha diritto ad una liquidazione inclusiva di tutto il danno non patrimoniale subìto, in proporzione alla durata ed intensità del vissuto, nonché alla composizione del restante nucleo familiare in grado di prestare assistenza morale e materiale, avuto riguardo all'età della vittima ed a quella dei familiari danneggiati, alla personalità individuale di costoro, alla loro capacità di reazione e sopportazione del trauma e ad ogni altra circostanza del caso concreto, da allegare e dimostrare (anche presuntivamente, secondo nozioni di comune esperienza) da parte di chi agisce in giudizio»

La Corte ha successivamente chiarito che in presenza della fattispecie della morte del congiunto può emergere sia il cd. "danno parentale"[24], sia il danno biologico[25] (quest'ultimo nel caso di degenerazione patologica medicalmente accertabile dello stato di sofferenza). È evidente che in questo caso la tutela della sfera relazionale dell'individuo si limita alle sole relazioni interumane. Altro discorso vale per le relazioni che esorbitino da questo paradigma.

Su tal fronte pare meritevole di un breve esame il filone giurisprudenziale che riguarda la risarcibilità del danno da morte dell'animale animale domestico, in cui si registra un tuttora perdurante contrasto tra giurisprudenza di legittimità[26], incline ad un atteggiamento tendenzialmente conservativo, e la

[22] Cass. 13 giugno 2017, 14655 in *Italgiure.*

[23] A seguito del celebre ciclo di pronunce costituito dalle famose sentenze di San Martino del 2008 (Cass. Civ. Sez. III, 12 dicembre 2008, n. 29191; Cass. Civ. Sez. III, 6 giugno 2008, n. 15029 entrambe in *Italgiure*) alla figura del danno non patrimoniale sono state ricondotte le tre sottovoci di danno (da non considerarsi quali sottocategorie autonome) del danno morale, come lesione «da sofferenza psichica o patema d'animo», il danno biologico, come «lesione temporanea o permanente all'integrità psicofisica suscettibile di accertamento medico-legale», danno esistenziale da intendersi come «alterazione della vita relazione e deterioramento complessivo della qualità di vita. (C. M. Bianca, *Trattato di Diritto Civile, V, La responsabilità*, Milano, 2012, 758).

[24] «In particolare, nel procedere all'accertamento ed alla quantificazione del danno [parentale] risarcibile, il giudice di merito deve valutare tanto l'aspetto interiore del danno sofferto (c.d. danno morale, sub specie del dolore, della vergogna, della disistima di sé, della paura, della disperazione) quanto quello dinamico-relazionale (destinato ad incidere in senso peggiorativo su tutte le relazioni di vita esterne del soggetto). Vi è da sottolineare che la misura standard del risarcimento prevista dalla legge o dal criterio equitativo uniforme adottato dagli organi giudiziari di merito può essere aumentata, nella sua componente dinamico-relazionale, solo in presenza di conseguenze dannose del tutto anomale ed eccezionali» Cass., Sez. III, 28 novembre 2018, n. 23469 in *Italgiure.*

[25] «Non costituisce duplicazione la congiunta attribuzione del danno biologico e di una ulteriore somma a titolo di risarcimento dei pregiudizi che non hanno fondamento medico-legale, perché non aventi base organica ed estranei alla determinazione medico-legale del grado di percentuale di invalidità permanente, rappresentati dalla sofferenza interiore (quali, ad esempio, il dolore dell'animo, la vergogna, la disistima di sé, la paura, la disperazione). Ne deriva che, ove sia dedotta e provata l'esistenza di uno di tali pregiudizi non aventi base medico-legale, essi dovranno formare oggetto di separata valutazione e liquidazione» Cass., Sez. III, 28 novembre 2018, n. 23469, riconfermata da Cass., Sez. III, 11 novembre 2019, n. 28989 in *Italgiure.*

[26] Cass., sez. III, 26 giugno 2007, n. 14846 in *DeJure* e, in seguito, Cass., sez. VI, ord. 23 ottobre 2018, n. 26770 in *Italgiure.*

giurisprudenza di merito, che, al contrario, si è mostrata disposta a più riprese ad avallare la tesi della piena riconoscibilità del danno non patrimoniale[27]. Una puntuale riflessione sulla vicenda sembra quanto mai opportuna, proprio in considerazione delle forti analogie, prospettate nella prima parte di questo lavoro, tra lo schema relazionale che oggi lega l'animale domestico all'uomo e quello che in futuro legherà quest'ultimo al robot. In ragione di queste analogie, infatti, il complessivo processo di riconoscimento del legame con l'animale domestico costituisce un importante banco di prova per il futuro riconoscimento di una ulteriore forma di relazione "non interumana" come quella con l'agente intelligente.

L'*iter* ragionativo della Corte prende le mosse da un primo arresto risalente al 2007[28] in cui la questione è così affrontata in esordio:

«la perdita… dell'animale da affezione, non sembra riconducibile sotto una fattispecie di un danno esistenziale consequenziale alla lesione di un interesse della persona umana alla conservazione di una sfera di integrità affettiva costituzionalmente protetta.»

Questa prima statuizione, che sembrerebbe escludere in radice la risarcibilità del danno esistenziale e, verosimilmente, *tout cort* del danno non patrimoniale, è tuttavia seguita da una seconda statuizione, che sembra portare il discorso verso una direzione diversa, e certamente meno univoca:

«La parte che domanda la tutela di tale danno, ha l'onere della prova sia per l'*an* che per il *quantum debeatur*, e non appare sufficiente la deduzione di un danno *in re ipsa*, con il generico riferimento alla perdita delle qualità della vita. Inoltre, la specifica deduzione del danno esistenziale impedisce di considerare la perdita, sotto un profilo diverso del danno patrimoniale (già risarcito) o del danno morale soggettivo e transeunte.»

L'argomentazione della Corte sembra qui virare sul tema della prova, evidentemente insufficiente sotto il profilo del danno esistenziale perché limitata ad un generico riferimento alla perdita della qualità di vita. Sorge a questo punto il dubbio sull'astratta configurabilità o meno del danno esistenziale, al di là del rilevato difetto di allegazione di parte. Per converso, sembra esplicitamente affermata la possibilità della configurazione del danno morale soggettivo, di cui certamente, in questo caso, è esclusa la risarcibilità per la mera strategia argomentativa del ricorrente.

L'orientamento riportato è stato ribadito, a distanza di ben undici anni dalla Suprema Corte in un arresto del 2018[29], che riproducendo parzialmente il passo riportato pronuncia del 2007 afferma che:

«non è riconducibile ad alcuna categoria di danno non patrimoniale risarcibile la perdita, a seguito di un fatto illecito, di un animale di affezione, in quanto essa non è qualificabile come danno esistenziale consequenziale alla lesione di un interesse della persona umana alla conservazione di una sfera di integrità affettiva costituzionalmente tutelata, non potendo essere sufficiente, a tal fine, la deduzione di un danno in *re ipsa*, con il generico

[27] Tra le varie, Trib. Venezia, 17 dicembre 2020, n. 1936; Trib. Parma, 2 maggio 2018, n. 605; Trib. Pavia, 16 settembre 2016, n. 1266; App. Torino, 29 ottobre 2012, n. 6296; Trib. Rovereto, 18 ottobre 2009, n. 499, tutte in *DeJure*.
[28] Cass., sez. III, 26 giugno 2007 n. 14846 in *DeJure*.
[29] Cass., sez. VI, ord. 23 ottobre 2018 n. 26770 in *ItalJure*.

riferimento alla perdita della "qualità della vita" ».

La portata del passo riportato mostra non trascurabili divergente rispetto alla precedente pronuncia. La prospettazione riguardante l'astratta configurabilità del danno morale soggettivo, ad esempio, sembra del tutto stralciata, dando l'impressione di una complessiva reinterpretazione della posizione precedente in senso maggiormente conservativo.

Tuttavia, la pronuncia si arricchisce di due ulteriori e importanti precisazione. Anzitutto rileva che:

«rispetto a tale arresto della giurisprudenza di legittimità, [del 2007] l'odierno ricorrente ha sostanzialmente omesso di confrontarsi in termini diretti, limitandosi ad esprimere unicamente il proprio dissenso attraverso il richiamo di precedenti giurisprudenziali di merito non adeguatamente argomentati, o di fonti normative da ritenersi non decisive o pertinenti».

E, soprattutto, che:

«l'eventuale (e invocata) rimeditazione del tema del danno patrimoniale da lesione dell'animale di affezione non risulta adeguatamente prospettata, in questa sede, in relazione alla (meno grave) ipotesi del suo ferimento (rispetto all'occorrenza dell'uccisione), vieppiù con specifico riguardo all'indicato pregiudizio delle ragioni non patrimoniali della persona danneggiata, apprezzabili sul piano dei valori e degli interessi di rilievo costituzionale concretamente compromessi».

Anche in questo caso la iniziale perentorietà nel tenore del discorso viene stemperata nel suo progredire. In sostanza, si afferma che – ferma restando l'attuale opinione negativa sulla questione sottoposta – una futura rimeditazione della posizione assunta sul tema non è da escludersi, a condizione che questa venga ispirata da un impianto argomentativo di parte ricorrente non limitato ad una "generica contestazione dei precedenti negativi in materia". In questo ultimo rilievo si può certamente scorgere un segno di apertura della Corte: l'orientamento riportato potrebbe mutare nel breve termine, (e magari conformarsi a quello delle Corti di altri Stati europei [30]), aprendo la strada al riconoscimento di nuove categorie relazionali. Al riportato orientamento bisogna, inoltre, contrapporre quello affermato dalle più recenti pronunce delle corti di merito. Le stesse hanno in diverse occasioni accordato il risarcimento del danno non patrimoniale da morte dell'animale da compagnia, sostenendo in via esplicita l'emersione, alla luce delle più recenti trasformazioni avvenute nell'ambito del comune sentire, di "un interesse della persona umana alla conservazione di una sfera di integrità affettiva costituzionalmente protetta"[31] desumibile dall'art 2 Cost.[32].

Spostando la prospettiva del discorso, non bisogna trascurare l'importante ruolo sociale che verranno in futuro a ricoprire i robot, soprattutto a favore

[30] Ad esempio, quello della Suprema Corte francese, la quale ha chiarito già da tempo l'ammissibilità del risarcimento del danno non patrimoniale per perdita dell'animale domestico, sempre a patto che (e qui si riscontrano assonanze con l'argomentare, anche se con esiti differenti di Cass., sez. III, 26 giugno 2007 n. 14846) la lesione del legame affettivo venga effettivamente provata. (Court d'Appel Lyon, 20 dècembre 2001, no de RG 1999/07446 citata da M.A. HERMITTE, *La nature, sujet de droit*?, in *Annales,* 2011, 175.

[31] Trib. Pavia, 16 settembre 2016, n. 1266 in *DeJure*.

[32] Trib. Venezia, 17 dicembre 2020, n. 1936; Trib. Pavia, 16 settembre 2016, n. 1266; App. Torino, 29 ottobre 2012, n. 6296; Trib. Rovereto, 18 ottobre 2009, n. 499 tutte in *DeJure*.

delle frange più deboli della popolazione[33]. Non bisogna dimenticare, infatti, che l'Intelligenza Artificiale, su cui si basa il funzionamento del robot, ha ancora oggi ampi margini di affinamento proprio sotto il profilo dell'interazione con l'individuo umano. Una volta preso atto di queste enormi potenzialità, sarà inevitabile interrogarsi sull'opportunità di estendere la "sfera relazionale tutelata dell'individuo" a cui si è fatto cenno nelle prime righe di questo paragrafo. Peraltro, questo risultato potrebbe addirittura essere promosso ad opera del legislatore, attraverso l'estensione di istituti giuridici su cui si fondano le relazioni sociali rilevanti per l'ordinamento. Come già accennato, autorevoli esponenti della dottrina hanno opportunamente evidenziato questa strada, che potrebbe forse portare ad un più immediato riconoscimento effettivo di questa categoria relazionale[34].

Se in ambito nazionale i segnali registrati sono ancora nel complesso non del tutto appaganti, in ambito europeo si segnala un panorama certamente più ricco. Per la verità, l'attenzione delle Istituzioni sembra riguardare più specificatamente la prevenzione dei risvolti negativi relativi al rapporto tra essere umano e robot. La criticità principale evidenziata dal Parlamento europeo risiede nella potenziale capacità dell'intelligenza artificiale di manipolare la "controparte" umana[35] al fine di indurla alla commissione di crimini. Questo rischio è stato evidenziato da uno studio (in verità piuttosto risalente) condotto sulla base dell'osservazione di interazioni tra essere umano ed I.A. L'ipotesi, in effetti, non pare affatto peregrina, soprattutto se si considera il crescente rischio di hackeraggio strettamente legato allo sviluppo futuro degli agenti intelligenti. Non solo: il potere persuasivo dei futuri robot, dotati di una vera e propria intelligenza relazionale, potrebbe essere utilizzato dallo stesso sviluppatore per influenzare le scelte del consumatore in senso a lui più svantaggioso[36]. Fenomeni legati alla sponsorizzazione di beni e servizi propri o di terzi veicolata attraverso la creazione più o meno artificiosa di un rapporto interpersonale diretto con il consumatore non appaiono affatto nuovi, ma sembrano piuttosto rinnovarsi in funzione dell'evoluzione delle tecnologie, come testimonia il recente successo dell'*influencing* sul web. La prevenzione di un simile rischio passa, ancora una volta, attraverso introduzione di obblighi di trasparenza che permettano alle autorità di verificare il funzionamento dell'algoritmo. Con riferimento al rischio dei soggetti più vulnerabili, in particolare, è stata avanzata la proposta di introdurre misure che rendano obbligatorio il *logging by design*, da intendersi come la registrazione all'interno di un supporto paragonabile ad una scatola nera, di ogni evento di interazione tra la macchina e il soggetto, in modo tale

[33] In particolare, con i soggetti anziani che già oggi si avvalgono dell'ausilio di assistenti-robot e mostrano in alcuni casi di stabilire legami di particolare intensità emotiva con essi (S. TURKLE, W. TAGGART, C. D. KIDD, & O. DASTÉ (2006). *Relational artifacts with children and elders: The complexities of cybercompanionship. Connection Science, 18*(4), 351).

[34] In particolare, L. GATT, nell'intervento citato, si interroga sulle sorti che toccherebbero alla trascrizione in Italia di matrimonio tra essere umano e robot celebrato in uno stato estero. Questo anche alla luce del fatto che gli esperti prevedono il sorgere in alcuni della disciplina dei matrimoni con i robot entro il 2050 (https://qz.com/871815/sex-robots-experts-predict-human-robot-marriage-will-be-legal-by-2050/).

[35] Parlamento europeo, *Report: The etichs of artificial intelligence: Issues and initiative*, 12 marzo 2020, 24.

[36] Proposta di regolamento del Parlamento Europeo e del Consiglio, 21 aprile 2021, *che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*. Vedi in particolare il divieto di cui all'art. 4, lettera (a) della Proposta.

da poter verificare ex post eventuali tentativi di manipolazione[37].

Conclusioni.

Tornando all'interno dei confini nazionali, e concludendo, sono stati esaminati in questo lavoro i più recenti studi condotti nell'ambito delle scienze sociali, al fine di ottenere indicazioni sulla natura di un futuro, nuovo, paradigma relazionale: quello tra individuo umano e agente intelligente (robot). Gli esiti di questo esame hanno portato a concludere che tale nuovo modello presenta forti profili di affinità con altre tipologie di relazione che nella realtà sociale risultano già pacificamente riconosciute: la relazione di tipo interumano e quella che lega l'individuo umano con l'animale da compagnia. Con riferimento a quest'ultima tipologia di relazione, è poi stata rilevata una discrepanza tra il suo (pacifico) riconoscimento all'interno della collettività e la sua effettiva tutela ordinamentale, almeno sotto lo specifico profilo del risarcimento del danno non patrimoniale da perdita dell'animale domestico. Sul punto, la recente posizione della Corte si mostra in ultima analisi aperta ad una futura revisione dell'attuale opinione (negativa) sul tema. Tale revisione, non potrà, evidentemente, che essere ispirata dalla stessa dottrina giuridica, la quale, forte della conoscenza a sua volta acquisite nel dialogo con le scienze sociali, dovrà portare argomentazioni decisive a favore del definitivo riconoscimento giuridico della relazione "non interumana" tra individuo e animale da compagnia. Una volta pervenuti a questo risultato, al netto di eventuali (e non escludibili) interventi del legislatore in tale ambito, un primo, fondamentale, passo in vista del futuro riconoscimento di altre relazioni "non interumane", e tra queste, per il caso che ci riguarda, la relazione tra robot e individuo umano, sarà definitivamente compiuto.

[37] Report from the Expert Group on Liability and New Technologies, 26 giugno 2019, *Liability for Atificial Intelligence,* 47, con specifico riferimento al caso di possibile manipolazione del minore da parte di giocattoli interattivi basati sull'intelligenza artificiale.

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

La tutela dell'utente degli strumenti di pagamento contro le transazioni fraudolente: problematiche giuridico-applicative e possibili evoluzioni.

User protection of payment instruments against fraudulent transactions: legal-application problems and possible evolutions.

LUIGI IZZO
Dottorando di ricerca *Sugli ambiti di interazione e integrazione tra le scienze umane e le tecnologie avanzate*, Università degli Studi di Napoli Suor Orsola Benincasa

Abstract

In circa trenta anni si è assistito a una evoluzione radicale del sistema finanziario, tanto nel panorama europeo quanto con riferimento a quello globale, mediante il processo di globalizzazione dei mercati, l'interconnessione delle economie, l'introduzione di una moneta unica a livello europeo, l'abbattimento delle frontiere nella prestazione dei servizi e lo sviluppo delle ICT (information and communications technologies).
Questi fenomeni, tra loro interconnessi, hanno innescato processi con conseguenze significative per numerosi ambiti, in particolare per quello dei servizi di pagamento., che ha visto la nascita e la diffusione della cd. "moneta elettronica".
Tuttavia, ciò ha portato con sé le inevitabili conseguenze negative, sostanziatesi nelle diverse e numerose metodologie di accesso truffaldino ai servizi di pagamento elettronici, tali da richiedere la predisposizione di sistemi a tutela dei titolari degli stessi, che non paiono essere idonei allo scopo dichiarato di proteggere i conti e i depositi, sovente violati da terzi.

In about thirty years there has been a radical evolution of the financial system, both in the European panorama and regarding the global one, through the process of globalization of the markets, the interconnection of economies, the introduction of a single currency at the European level, the abolition of borders in the provision of services and the development of ICT (information and communications technologies).
These phenomena, interconnected with each other, have triggered processes with significant consequences for numerous areas, in particular for that of payment services., Which saw the birth and spread of the so-called "Electronic money".
However, this has brought with it the inevitable negative consequences, resulting in the various and numerous methods of fraudulent access to electronic payment services, such as to require the preparation of systems to protect the holders of the same, which do not appear to be suitable for the declared purpose of protect accounts and deposits, often violated by third parties.

Parole chiave: Strumenti di pagamento; moneta elettronica; ICT; Data Protection.

Keywords: payment instruments; e-money; ICT; Data Protection.

Introduzione.

La cd. "moneta elettronica", altrimenti detta *e-money*[1] in correlazione al fenomeno del commercio elettronico, ossia l'*e-commerce*, è una delle innovazioni più importanti nell'ambito delle transazioni bancarie, basata sul concetto di trasferimento di somme di denaro slegato dalla materialità della consegna e attuato a mezzo di impulsi elettronici. In verità, tale modalità di pagamento era già molto diffusa prima dell'attuale crisi pandemica globale, per quanto quest'ultima abbia determinato un ricorso sempre più intenso ai sistemi di pagamento dematerializzati[2]. Tuttavia, se è vero che circa nove milioni di italiani sono oramai avviati sulla strada dei pagamenti digitali (anche per le piccole spese quotidiane), è altrettanto vero che ben diciotto milioni sono coloro che, per svariati motivi, rinunziano ad abbracciare (in parte o totalmente) la strada della digitalizzazione e tra le motivazioni risalta il timore di essere oggetto di furti e clonazioni (16,8% degli intervistati)[3].

Tale paura non è assolutamente infondata, anzi. Si può tranquillamente

[1] L'espressione è usata in P. PACILEO, *L'attuazione in Italia delle direttive comunitarie in materia di e-money*, in *La moneta elettronica: profili giuridici e problematiche applicative*, a cura di SICA-STANZIONE-Z. ZENCOVICH, Giuffrè, 2006, p. 191.

[2] Si consideri che nel commercio e nei pagamenti si attuano operazioni che vengono svolte (ancora, per ora) toccando, prendendo, usando oggetti che, spesso e volentieri, cambiano possesso più volte nel corso della stessa giornata. Ma proprio per questo si è verificato un forte ricorso al digitale, attesa l'incompatibilità di simili procedure fisiche in ragione della perdurante pandemia da SARS-CoV-2. Anche l'utilizzo del denaro contante, ovviamente, ha risentito di simili tendenze, per quanto, in questo specifico caso, parte della "colpa" sia da rinvenirsi più in una certa "informazione giornalistica" condotta male e che ha dominato la prima parte della pandemia (cfr. B. GARDNER, *Dirty banknotes may be spreading the coronavirus, WHO suggests*, articolo comparso il 2 marzo 2020 su www.telegraph.co.uk/news/2020/03/02/exclusive-dirty-banknotes-may-spreading-coronavirus-world-health/. L'articolo in questione, per l'autorevolezza della testata, è stato immediatamente ripreso da diversi giornali in tutto il mondo, con conseguenze facilmente immaginabili). Questa tendenza è stata poi confermata in occasione della presentazione della nuova edizione dell'Osservatorio Innovative Payments della School of Management del Politecnico di Milano, avvenuta durante l'evento «*Innovative Payments: da alternativa a necessità*», nella quale risulta che un terzo degli acquisti effettuati dagli italiani è avvenuto per mezzo dei sistemi di pagamento elettronici (cfr. A. LAR., *Covid e cashback spingono i pagamenti digitali: nel 2020 senza contanti un acquisto su tre*, 11 marzo 2021 su www.ilsole24ore.com/art/covid-e-cashback-spingono-pagamenti-digitali-nel-2020-senza-contanti-acquisto-tre-ADPXnZPB).

[3] L. INCORVATI, *La paura del contagio porta a dire addio al contante*, 22 ottobre 2020 su www.ilsole24ore.com/art/la-paura-contagio-porta-dire-addio-contante-ADaCrZx

asserire che, in parallelo con la diffusione dei servizi di pagamento digitali, si è avuta una sempre più alta circolazione di truffe e attacchi informatici quali *phishing*, SIM *Swap* e clonazione, a danno dei sistemi di pagamento come le carte di credito.

Ovviamente, il *trend* pare destinato unicamente ad acuirsi. Tant'è vero che da un rapporto statistico relativo al nostro Paese, pubblicato nel 2020 dal Ministero dell'Economia e delle Finanze (MEF)[4] e aggiornato al 2019, emerge testualmente che «Le frodi, sia in valore che in numero, sono in forte aumento rispetto all'anno precedente (circa +28%). Quelle in valore sono dunque salite a un livello leggermente superiore (102,3) rispetto a quello del 2009, mentre quelle in numero si mantengono molto più elevate (207,1). In termini di valore, senza tenere conto delle transazioni totali genuine, si assiste a un aumento del fenomeno su tutti i canali. Nello specifico, colpisce l'incremento dei prelievi ATM (+44,1%), accompagnato da un incremento del 27,6% sul canale Internet e del 25% su POS. La maggior parte delle frodi su Internet risulta avvenuta all'estero.»[5].

Un simile aumento non deve certo stupire, anche in considerazione di come i malviventi abbiano a disposizione una variegata panoplia di strumenti per perpetrare le loro frodi. In generale, tali metodi atti a frodare vengono suddivisi in due macrocategorie:

- La macrocategoria delle frodi CNP, acronimo con cui si intende una transazione del tipo "*card-not-present*", ossia che prescinde dall'utilizzo di una carta di pagamento per l'autenticazione dell'utente, dovendosi "solo" inserire, seguendo le indicazioni del sistema che gestisce il pagamento, il codice CCV, il numero della carta, il PIN ovvero un codice monouso fornito dal proprio intermediario a mezzo SMS o tramite apposita app. Pertanto, rientrano in questa categoria tutte le transazioni che avvengono su store online, su servizi di home banking, su sistemi di tipo e-wallet. Ovviamente, nell'ipotesi di frode il soggetto che inserisce manualmente i dati in questione non è assolutamente identificabile con il titolare dello strumento di pagamento;
- La macrocategoria delle frodi "materiali", attuate tramite terminali ATM e POS vedono una modifica dei dispositivi che leggono le carte in modo da carpirne i dati, uniti a microtelecamere per vedere la digitazione del PIN, così da utilizzarli per clonare materialmente le carte e successivamente utilizzarle.

Tuttavia, la modifica dei dispositivi può risultare oggettivamente rischiosa da operare [6] e, invero, sono oramai sono comunemente diffusi una serie di

[4] MEF – DIPARTIMENTO DEL TESORO, *Rapporto statistico sulle frodi con le carte di pagamento 2020*, a cura della DIREZIONE V UFFICIO VI – UCAMP – UFFICIO CENTRALE ANTIFRODE DEI MEZZI DI PAGAMENTO, disponibile al link http://www.dt.mef.gov.it/modules/documenti_it/antifrode_mezzi_pagamento/antifrode_mezzi_pagamento/Rapporto_statistico_sulle_frodi_con_le_carte_di_pagamento_-_edizione_2020.pdf

[5] *Ivi*, p. 7-8

[6] Si consideri, a titolo esemplificativo, una tecnica alquanto "artigianale" e, per questo, ben più rischiosa, definita "*lebanese loop*". Questa consiste nella manomissione della sola fessura di inserimento della carta di un ATM, inserendo nella stessa un dispositivo che blocca fisicamente la carta di pagamento (cfr. https://www.axisbank.com/bank-smart/safe-banking/atm/lebanese_loop.html). In quel momento, poi, il malcapitato, generalmente un anziano, viene avvicinato da un soggetto che, guarda caso, transitava nelle vicinanze e si poneva subito a disposizione dell'utente al solo scopo di carpire il codice PIN, in modo da utilizzarlo con la carta di pagamento originale, che avrebbe estratto in seguito all'allontanamento del

comportamenti prudenziali[7] a scopo di contrasto.

Ne consegue che le tecniche tipo CNP dominano letteralmente le statistiche di settore. Di queste tecniche, certamente la più conosciuta e diffusa è quella del *phishing*[8], una forma di adescamento della quale numerosi cadono vittime grazie a un abile sfruttamento delle loro stesse paure.

Per esempio, per mezzo di una mail ovvero di un SMS (nel qual caso si parla di *smishing*) si viene avvisati di un supposto problema relativo al nostro account, solitamente legato alla sicurezza. Magari in tale comunicazione si avverte l'utente di un blocco (ovviamente inventato) dell'account e per risolverlo invita a cliccare su un link che, però, riporta a un sito fittizio, controllato dal cracker e che riproduce molto bene il portale dell'istituto bancario o della posta, rendendo difficile rendercisi conto di quel che si sta facendo.

In tal modo, senza rendersi conto che li sta letteralmente regalando al criminale, l'utente ingenuamente inserisce i dati sensibili relativi alla propria carta di pagamento in quelli che sembrano i campi di compilazione di una pagina apparentemente appartenente al proprio intermediario.

Non solo mail e SMS sono i vettori di queste frodi, dal momento che sono divenute ancora più insidiose grazie all'utilizzo del *vishing* (ossia il *voice-phishing*), che è attuato a mezzo telefonate da parte di presunti operatori che avvertono (o meglio, allarmano) l'utente in merito a non meglio dichiarate anomalie delle carte di pagamento[9].

Poi, a testimoniare l'evoluzione delle frodi CNP, si può ricordare anche l'*e-skimming*[10] (che prende ispirazione da una tecnica descritta nel prossimo paragrafo) e che, mediante l'installazione di codice malevolo nelle pagine *web* in cui erano presenti moduli da compilare per effettuare pagamenti online, provocava una "sostituzione" di questi moduli compilabili con altri predisposti dai cybertruffatori e che avrebbero trasmesso a questi i dati inseriti dagli utenti.

Ciò conduce necessariamente a chiedercisi se, contro simili minacce, l'attuale sistema di tutele sia adeguato ovvero necessiti di essere rivisto.

---

legittimo titolare, convinto di aver perso la carta e di doverla far estrarre fisicamente dall'ATM ad opera dei tecnici della filiale (cfr. A. ZURLO, *La truffa del cd. "lebanese loop" - Nota a ABF, Collegio di Roma, 11 gennaio 2021, n. 540*, su www.dirittodelrisparmio.it).

[7] Vedasi quelli descritti in una pagina del sito istituzionale dei Carabinieri, disponibile al link http://www.carabinieri.it/cittadino/consigli/tematici/giorno-per-giorno/la-carta-di-credito/carta-di-credito

[8] R. RIJTANO, *Phishing, cos'è e come proteggersi: la guida completa*, 29 maggio 2018 su www.cybersecurity360.it. Ma si considerino pure le pagine ad essa dedicate dai vari intermediari, quali Intesa San Paolo (https://www.intesasanpaolo.com/it/common/landing/anti-phishing/phishing-vishing-smishing-come-proteggersi.html) e Poste Italiane (https://www.poste.it/psd2-e-sicurezza---come-difendersi-dalle-truffe.html). Secondo la giurisprudenza penale (cfr. *ex multis* Trib. Monza, 7 maggio 2009, in *Riv. pen.*, 2010) tale condotta è configurabile anche mediante intrusione nel sistema informatico ed è sussumibile nella fattispecie di "truffa", come pure quella di accesso abusivo in sistema informatico (cfr. PERRI, *Analisi informatico-giuridica dei reati di frode informatica e accesso abusivo a un sistema informatico o telematico con l'aggravante dell'abuso della qualità di operatore del sistema*, in *Giur. merito*, 2008, 1651).

[9] REDAZIONE, *La nuova cybertruffa in auge è il vishing*, 30 maggio 2020 su www.ilsole24ore.com

[10] S. LOMBARDO, *E-skimmer nascosti nei siti Web, così ci clonano le carte di credito: che c'è da sapere*, 14 maggio 2020 su www.cybersecurity360.it

1. Il quadro normativo europeo e nazionale.

Al fine di analizzare compiutamente l'attuale scenario sul piano giuridico, non è possibile prescindere da una previa analisi della normativa di riferimento e va chiarito, anzitutto, cosa sia la "moneta elettronica" e quali ipotesi di responsabilità siano state previste dal legislatore tanto per l'utente della stessa e degli strumenti che di essa si avvalgono quanto per l'intermediario che la fornisce.

1.1 Il concetto di "moneta elettronica".

Trattasi di espressione che, in verità, è oramai datata, poiché coniata all'inizio del processo di rinnovamento dei sistemi di pagamento, i quali sono attualmente arrivati a quella che sarebbe la quarta generazione degli stessi[11]. Infatti, questo concetto fa la sua comparsa per la prima volta in un testo normativo europeo con la Raccomandazione della Commissione 97/489/CE del 30 luglio 1997 "*relativa alle operazioni mediante strumenti di pagamento elettronici, con particolare riferimento alle relazioni tra gli emittenti ed i titolari di tali strumenti*", dove si legge testualmente, nel terzo Considerando, «*che ai fini della presente raccomandazione, gli strumenti di pagamento comprendono inoltre gli strumenti di moneta elettronica ricaricabili aventi forma di carte con valore immagazzinato e di memorie di elaboratori elettronici collegati in rete*»[12].

Il primo atto effettivamente vincolante in tale ambito è, piuttosto, la prima Direttiva IMEL (così denominata perché introduce, accanto ai classici intermediari, anche gli Istituti di Moneta Elettronica, gli IMEL), attuata in Italia con il d.lgs. n. 39/2002 e il cui terzo Considerando qualifica la moneta elettronica come un *surrogato elettronico* del normale denaro contante[13].

Tale Direttiva è stata poi superata dalla seconda Direttiva IMEL[14], recepita dal nostro Legislatore con il d.lgs. n. 45/2012 e nella quale viene indicato come prioritario un aggiornamento della definizione stessa di "moneta elettronica", tant'è vero che nei Considerando dell'atto – elementi imprescindibili al fine di

---

[11] P. SPADA, *Carte di credito, terza generazione dei mezzi di pagamento*, in *Rivista di Diritto Civile*, 1976, I, pag. 489, dove la prima generazione dei mezzi di pagamento è identificata con la moneta avente corso legale, la seconda nei titoli di credito, la terza nelle carte di credito. Pertanto, molto probabilmente, la quarta potrebbe essere ragionevolmente rappresentata dagli attuali trasferimenti elettronici di fondi e nei pagamenti elettronici.

[12] Invero, vi è chi fa notare come questa espressione sia ancor più risalente nel tempo (cfr. L. CAPALDO, *Moneta elettronica e trasparenza, in La moneta elettronica: profili giuridici e problematiche applicative*, a cura di SICA-STANZIONE-Z. ZENCOVICH, Giuffrè, 2006, p. 158). in quanto rinvenibile nel report del 1996 *SECURITY OF ELECTRONIC MONEY*, stilato a cura del *Committee on Payment and Settlement System* (disponibile su www.bis.org/cpmi/publ/d18.pdf). Vi è poi il GUERRIERI (cfr. G. GUERRIERI, *La moneta elettronica – profili giuridici dei nuovi sistemi di pagamento*, Il Mulino, 2015, p. 41 nota n. 2) che la retrodata ulteriormente al 1994, anno in cui fu presentato il "*Report to the Council of the European Monetary Institute on prepaid cards*" (disponibile su www.ecb.europa.eu/pub/pdf/other/prepaidcards1994en.pdf), nel quale si parla, molto profeticamente, di *cashless money* (pag. 9) ed *electronic purse money* (pag. 6).

[13] Direttiva 2000/46/CE "*riguardante l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica*", art. 1, co. 2, lett. b), dove si definisce la "moneta elettronica" come «*un valore monetario rappresentato da un credito nei confronti dell'emittente che sia: i) memorizzato su un dispositivo elettronico; ii) emesso dietro ricezione di fondi il cui valore non sia inferiore al valore monetario emesso; iii) accettato come mezzo di pagamento da imprese diverse dall'emittente.*»

[14] Direttiva 2009/110/CE, "*concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE*"

fornire una chiave di lettura preziosa per risolvere le ambiguità che spesso sono presenti nel testo legislativo[15] – si asserisce che «*(7) È opportuno introdurre una definizione chiara di moneta elettronica che sia tecnicamente neutra. […]. (8) È opportuno che la definizione di moneta elettronica copra la moneta elettronica, sia se detenuta su un dispositivo di pagamento in possesso del detentore di moneta elettronica, sia se memorizzata a distanza su un server e gestita dal detentore tramite un conto specifico per la moneta elettronica. Tale definizione dovrebbe essere abbastanza generale da non ostacolare l'innovazione tecnologica e da includere non soltanto tutti i prodotti di moneta elettronica disponibili oggi sul mercato, ma anche i prodotti che potrebbero essere sviluppati in futuro.*».

1.2 I profili di responsabilità previsti in tema di *e-money*.

Chiarita la nozione base di *e-money*, si procede ad illustrare il regime di responsabilità delineato a mezzo delle ultime novelle legislative.

Questi profili sono stati disciplinati per mezzo di separati atti comunitari, ossia le due Direttive sui sistemi di pagamento (PSD1[16] e PSD2[17]), le cui innovazioni sono confluite tutte nel d.lgs. n. 11/2010.

Innanzitutto, è necessario separare la responsabilità dell'emittente della moneta elettronica da quella che si pone in capo all'utilizzatore della stessa, la quale è disciplinata dall'art. 7 del d.lgs. n. 11/2010, relativo agli obblighi dell'utente della Moneta Elettronica[18]. Secondo questa disposizione, l'utente ha, sostanzialmente, due obblighi, di cui il primo configurabile come obbligo di *comunicazione* e il secondo quale obbligo di *custodia* e di *uso conforme* dello strumento di pagamento.

È a detti obblighi che si ricollega l'art. 12[19], il quale disciplina appunto la

---

[15] R. Baratta, *Complexity of EU law in the domestic implementing process*, articolo tra gli atti del seminario *Quality of legislation - EU Legislative Drafting: Views from those applying EU law in the Member States*, tenutosi a Bruxelles il 3 luglio 2014 e disponibile su ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf, p. 13, laddove si ricorda come «*Recitals can help to explain the purpose and intent behind a normative instrument. They can also be taken into account to resolve ambiguities in the legislative provisions to which they relate*». Ciononostante, valga l'avvertimento della Corte di Giustizia dell'Unione Europea che ricorda come questi Considerando non abbiano «*binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the act in question*» (cfr. Case C-162/97, Nilsson, [1998] ECR I-7477, para. 54, disponibile su https://eur-lex.europa.eu).

[16] Direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE (*Payment Services Directive*)

[17] Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE

[18] «*1. L'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di: a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso e che devono essere obiettivi, non discriminatori e proporzionati; b) comunicare senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza.*

2. Ai fini di cui al comma 1, lettera a), l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate.».

[19] «*1. Salvo il caso in cui abbia agito in modo fraudolento, l'utente non sopporta alcuna perdita derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente intervenuto dopo la comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera b).*

responsabilità del pagatore, valutabile sotto tre profili:

- Che abbia agito con intenti fraudolenti nei confronti dell'emittente di moneta elettronica[20];
- Che abbia dolosamente omesso di adempiere agli obblighi di custodia dello strumento di pagamento;
- Che abbia, con colpa grave, omesso di adempiere compiutamente agli obblighi di custodia dello strumento di pagamento.

Ora, se nei primi due casi è possibile, in qualche modo, qualificare il "livello" di imputabilità della relativa condotta, più difficile è, invece, definire quando si sia in presenza di colpa grave ovvero di colpa lieve/assente.

In tal caso, si dovrà avere riguardo al contenuto delle disposizioni contrattuali, le quali, spesso e volentieri, sono fornite di esempi che chiariscono la condotta da tenersi[21].

Per contro, la responsabilità del *provider* di servizi di pagamento appare definita in modo molto meno articolato. Si consideri quanto previsto nell'art. 8, d.lgs. n. 11/2010:

«1. Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di:

a) assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7;

b) astenersi dall'inviare strumenti di pagamento non richiesti, a meno che lo strumento di pagamento già consegnato all'utente debba essere sostituito;

c) assicurare che siano sempre disponibili strumenti adeguati affinché l'utente dei servizi di pagamento possa eseguire la comunicazione di cui all'articolo 7, comma 1, lettera b), nonché, nel caso di cui all'articolo 6, comma 4, di chiedere lo

---

2. Salvo il caso in cui abbia agito in modo fraudolento, l'utente non è responsabile delle perdite derivanti dall'utilizzo dello strumento di pagamento smarrito, sottratto o utilizzato indebitamente quando il prestatore di servizi di pagamento non ha adempiuto all'obbligo di cui all'articolo 8, comma 1, lettera c).

2-bis. Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente.

2-ter. Il pagatore non sopporta alcuna perdita se lo smarrimento, la sottrazione o l'appropriazione indebita dello strumento di pagamento non potevano essere notati dallo stesso prima di un pagamento, salvo il caso in cui abbia agito in modo fraudolento, o se la perdita è stata causata da atti o omissioni di dipendenti, agenti o succursali del prestatore di servizi di pagamento o dell'ente cui sono state esternalizzate le attività.

3. Negli altri casi, salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita.

4. Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3.».

[20] Trattasi dei casi in cui il cliente operi una falsa denuncia di operazioni non autorizzate ovvero eseguite in modo inesatto, trasmettendo una comunicazione ai sensi dell'art. 9, d.lgs. n. 11/2010

[21] Per esempio, si considerino le Condizioni Generali della FinecoBank S.p.A., aggiornate al 18 marzo 2021 e disponibili al link https://images.fineco.it/pub-fineco/pdf/apriconto/condizioni_generali.pdf, nello specifico il contenuto degli artt. 4, rubricato "Custodia della Carta e del P.I.N. e del Codice di Sicurezza", e 5, inerente all'ipotesi di smarrimento/sottrazione delle credenziali. Ebbene, avendo quale riferimento un ipotetico caso con, quale "protagonista", un cliente della FinecoBank S.p.A., si dovrà innanzitutto verificare se la sua condotta sia stata aderente alle raccomandazioni presenti nello stesso testo contrattuale o meno, così da poter verificare se si sia quantomeno nell'ambito della cd. "colpa grave" ai fini di una imputabilità, nei confronti dell'utente, delle conseguenze negative delle operazioni di cui questi chiede il rimborso.

sblocco dello strumento di pagamento o l'emissione di uno nuovo, ove il prestatore di servizi di pagamento non vi abbia già provveduto. Ove richiesto dall'utente, il prestatore di servizi di pagamento gli fornisce i mezzi per dimostrare di aver effettuato la comunicazione di cui all'articolo 7, comma 1, lettera b), entro i 18 mesi successivi alla comunicazione medesima;

c-bis) fornire all'utente la possibilità di procedere alla comunicazione di cui all'articolo 7, comma 1, lettera b), a titolo gratuito, addebitandogli eventualmente solo i costi di sostituzione dello strumento di pagamento;

d) impedire qualsiasi utilizzo dello strumento di pagamento successivo alla comunicazione di cui all'articolo 7, comma 1, lettera b).

2. I rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate sono a carico del prestatore di servizi di pagamento.».

Quindi, pure il *provider* è soggetto a degli obblighi, solo che sembrano essere limitati piuttosto alla "semplice" garanzia dell'integrità dei dati in suo possesso, da intendersi tanto come condotta volta a prevenire intrusioni nel sistema informatico quanto come condotta idonea, *ex post*, a porre rimedio ad eventuali anomalie[22].

E, invero, i profili di responsabilità previsti all'art. 11, d.lgs. n. 11/2010 sono strettamente attinenti alla custodia del sistema informatico in sé, stante il fatto che le ipotesi di utilizzo fraudolento ovvero omissione colposa/dolosa delle precauzioni in tema di custodia sono chiaramente definite nel successivo art. 12, delineato in precedenza. Infatti, se si considera che l'art. 11[23] non delinea

---

[22] R. CELELLA, *Principi generali della protezione dei dati personali: qualità e integrità dei dati*, su *www.dataprotectionlaw.it*, 15 luglio 2018

[23] Art. 11, d.lgs. n. 11/2010 - «*1. Fatto salvo l'articolo 9, nel caso in cui sia stata eseguita un'operazione di pagamento non autorizzata, il prestatore di servizi di pagamento rimborsa al pagatore l'importo dell'operazione medesima immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito. Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo.*

2. In caso di motivato sospetto di frode, il prestatore di servizi di pagamento può sospendere il rimborso di cui al comma 1 dandone immediata comunicazione per iscritto alla Banca d'Italia all'((...)).

2-bis. Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, il prestatore di servizi di pagamento di radicamento del conto rimborsa al pagatore immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, l'importo dell'operazione non autorizzata, riportando il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo. In caso di operazione di pagamento non autorizzata, se il relativo ordine di pagamento è disposto mediante un prestatore di servizi di disposizione di ordine di pagamento, quest'ultimo è tenuto a rimborsare immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, senza che sia necessaria la costituzione in mora, al prestatore di servizi di pagamento di radicamento del conto su richiesta di quest'ultimo, gli importi rimborsati al pagatore. Se il prestatore di servizi di disposizione di ordine di pagamento è responsabile dell'operazione di pagamento non autorizzata, risarcisce immediatamente e, in ogni caso, entro la fine della giornata operativa successiva senza che sia necessaria la costituzione in mora il prestatore di servizi di pagamento di radicamento del conto, su richiesta di quest'ultimo, anche per le perdite subite. In entrambi i casi è fatta salva la facoltà del prestatore di servizi di disposizione di ordine di pagamento di dimostrare, in conformità a quanto disposto dall'articolo 10, comma 1-bis, che, nell'ambito delle sue competenze, l'operazione di pagamento è stato autenticato, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti relativi al servizio di pagamento da questo prestato, con conseguente diritto in questi casi alla restituzione delle somme da quest'ultimo versate al prestatore di servizi di pagamento di radicamento del conto ai sensi del presente comma.

3. Il rimborso di cui ai commi precedenti non preclude la possibilità per il prestatore di servizi di pagamento di dimostrare, anche in un momento successivo, che l'operazione di pagamento era stata autorizzata. In tal caso, il

chiare ipotesi a carico del prestatore di servizi di pagamento, mentre, al contrario, sono precisamente descritte quelle previste a carico dell'utente del sistema di pagamento, ne consegue logicamente che, per esclusione, tutte quelle possibili fattispecie di responsabilità non ricomprese (e non ricomprendibili) nel disposto dell'art. 12 vanno intese come rientranti nel campo di applicazione dell'art. 11[24].

1.3 I presidi di sicurezza adottati dopo la PSD2.

Spostando ora l'attenzione sui metodi di autenticazione, va chiarito che questi non si riducono unicamente alla combinazione PIN/striscia magnetica – come nel caso di pagamenti con POS o prelievi presso gli ATM – ovvero all'utilizzo dei dati presenti sulla carta, magari in combinazione con i normali dati di autenticazione utilizzati per l'accesso al portale di *home banking* del proprio intermediario (*password* o indirizzo *e-mail* di riferimento)[25].

Infatti, è stato adottato un differente approccio, consacrato con la Direttiva PSD2, il quale sfocia nell'adozione della cd. "*Strong Customer Authentication*" (d'ora in avanti SCA) in relazione a qualsiasi operazione avvenga *online*[26].

In virtù del Regolamento di attuazione di questa Direttiva, quindi "*l'autenticazione si basa su due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza e comporta la generazione di un codice di autenticazione.*"[27], peraltro indipendenti tra loro e interscambiabili, in modo tale che la violazione di uno di questi tre fattori di autenticazione non comporti l'automatica compromissione degli altri due[28]. Questi tre elementi tra cui è possibile scegliere sono:

– identificazione con una password o con un PIN: quindi qualcosa di criptato che l'utente *conosce* [29] può essere una parola chiave

---

prestatore di servizi di pagamento ha il diritto di chiedere direttamente all'utente e ottenere da quest'ultimo la restituzione dell'importo rimborsato ai sensi dei commi 1 e 2-bis.
4. Il risarcimento di danni ulteriori subiti può essere previsto in conformità alla disciplina applicabile al contratto stipulato tra l'utente e il prestatore di servizi di pagamento compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento.»

[24] G. Guerrieri, *La moneta elettronica – profili giuridici dei nuovi sistemi di pagamento*, cit., p. 158, dove pone, quale esempio, l'ipotesi di un malfunzionamento proprio del sistema informatico, tale da comportare una "duplicazione" della medesima operazione di pagamento, la quale venga effettuata due volte, senza che vi sia responsabilità alcuna del pagatore

[25] Per i quali, tra l'altro, valgono i normali "presidi di sicurezza" identificabili come le misure dettate dal buon senso e descritte dalla Banca d'Italia al link https://economiapertutti.bancaditalia.it/notizie/pagamenti-in-sicurezza/

[26] Art. 10-*bis*, co. 1, d.lgs. n. 11/2010 – "*Conformemente all'articolo 98 della direttiva (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente:*
a) accede al suo conto di pagamento on-line;
b) dispone un'operazione di pagamento elettronico;
c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi."

[27] Art. 4 del Regolamento Delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri

[28] Art. 9 del Regolamento Delegato (UE) 2018/389

[29] Art. 6 del Regolamento Delegato (UE) 2018/389 – "*1. I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come* ***conoscenza*** *siano acquisiti da soggetti non autorizzati o divulgati a questi ultimi. 2. L'uso di detti elementi da parte del*

piuttosto che un codice o una domanda di sicurezza;
- identificazione con qualcosa che sia in *possesso*[30] all'utente e che l'utente può utilizzare, tipicamente un device come lo smartphone piuttosto un device portatile o ancora un token bancario;
- identificazione con qualcosa di fisico: impronta digitale o lineamenti biometrici del viso, ovvero tratti che, in qualche modo, sono *in grado di caratterizzare il cliente*[31] identificandolo nella sua persona in modo univoco.

Per esempio, laddove si intenda acquisire un biglietto del treno a mezzo *PayPal*, si dovrà in primo luogo inserire il primo fattore di autenticazione, che è quello che dà accesso al servizio stesso di *PayPal*, per poi inserire il secondo fattore di autenticazione, fornito direttamente dall'intermediario che gestisce la carta di pagamento collegata all'*e-wallet*.

Di conseguenza, nel caso di acquisti *online* sarà necessario utilizzare questa autenticazione forte, seguendo una regola particolarmente rigida.

Ebbene, va riconosciuto che la stessa opera indubbiamente a vantaggio sia dei consumatori che degli esercenti di *e-commerce*, in quanto consente di tenere sotto controllo pressoché qualsiasi movimento di fondi sui propri mezzi di pagamento elettronici, con delle esenzioni ben tipizzate.

Tuttavia, queste nuove procedure in materia di autenticazione non paiono aver sortito pienamente l'effetto sperato (anzi, sono pure contestate dagli esercenti in quanto disincentiverebbero gli acquirenti dal proseguire acquisti già iniziati[32]).

Tale risultato è da attribuirsi all'evoluzione costante delle tecniche con cui ci si appropria delle credenziali di accesso ai sistemi di pagamento a fini fraudolenti[33].

---

pagatore è soggetto a misure di attenuazione allo scopo di impedire che vengano divulgati a soggetti non autorizzati."

[30] Art. 7 del Regolamento Delegato (UE) 2018/389 – "*1. I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come* ***possesso*** *siano utilizzati da soggetti non autorizzati. 2. L'uso di detti elementi da parte del pagatore è soggetto a misure volte a impedirne la duplicazione.*"

[31] Art. 8 del Regolamento Delegato (UE) 2018/389 – "*1. I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi di autenticazione classificati come* ***inerenza*** *e letti dai dispositivi e dal software di accesso forniti al pagatore siano acquisiti da soggetti non autorizzati. Come minimo, i prestatori di servizi di pagamento garantiscono che la probabilità che soggetti non autorizzati effettuino l'autenticazione a nome del pagatore utilizzando detti dispositivi e software sia molto bassa. 2. L'utilizzo di detti elementi da parte del pagatore è soggetto a misure volte ad assicurare che detti dispositivi e software garantiscano la resistenza contro l'utilizzo non autorizzato degli elementi mediante l'accesso ai dispositivi e al software.*"

[32] Infatti, una ricerca condotta dalla AXERVE S.P.A., società operante nel settore dei pagamenti digitali, sulla base di dati forniti da Mastercard, fa emergere come siano numerose le transazioni che non vengono concluse a causa di *timeout* di sistema ovvero di disagi sul piano della *user experience* – cfr. A. S., *E-commerce, transazioni più sicure grazie all'analisi in real time*, 3 maggio 2021 su www.pagamentidigitali.it

[33] Per esempio, si consideri la tecnica definita "SIM Swap", con cui il truffatore cambia il numero di telefono del titolare con il proprio, al fine di "bucare" i sistemi SCA che sfruttano l'elemento della conoscenza unito a quello del possesso. Cfr. S. GALEOTTI, *Truffa sim swap, le banche: "L'addio alle chiavette token ha aumentato sicurezza. I clienti devono essere più attenti al phishing"*, 31 gennaio 2020 su www.ilfattoquotidiano.it dove sono riportate le dichiarazioni in materia del Segretario Generale di ABI Lab (www.abilab.it/web/guest/chi-siamo), il centro di ricerca promosso dall'ABI (Associazione Bancaria Italiana).

2. Problematiche in tema di responsabilità degli intermediari.

Chiarito, quindi, come siano disciplinate le ipotesi di responsabilità per i soggetti parte del rapporto contrattuale inerente alla gestione dello strumento di pagamento e quali siano i presidi di sicurezza adottati, è necessario ora delineare brevemente gli orientamenti formatisi nel nostro Ordinamento in relazione specificamente alla responsabilità dell'intermediario, sia nell'ambito della giurisprudenza (arbitrale e ordinaria) sia nell'ambito della dottrina.

Ciò in quanto sussiste un chiaro *favor* verso l'utente dei sistemi di pagamento, come risulta dai Considerando della Direttiva PSD2[34].

2.1 I primi orientamenti in materia di diligenza bancaria tra dottrina e giurisprudenza.

Invero, è bene considerare che in ambito dottrinale, spesso e volentieri, sono state precorse le successive elaborazioni giurisprudenziali.

Più nello specifico, è necessario considerare quanto scritto in tema di

[34] Si consideri per esempio quanto disposto nei Considerando 91, 95 e 96 di detta Direttiva: «*(91) I prestatori di servizi di pagamento sono responsabili delle misure di sicurezza. Tali misure devono essere proporzionate ai relativi rischi di sicurezza. È opportuno che i prestatori di servizi di pagamento stabiliscano un quadro per attenuare i rischi e mantenere procedure efficaci di gestione degli incidenti. È opportuno mettere in atto un meccanismo di segnalazione periodica in modo da garantire che i prestatori di servizi di pagamento forniscano periodicamente alle autorità competenti una valutazione aggiornata dei rischi di sicurezza cui sono confrontati e delle misure che hanno adottato per contrastarli. Inoltre, affinché i danni agli utenti, ad altri prestatori di servizi di pagamento o ad altri sistemi di pagamento, tra cui disfunzioni sostanziali di un sistema di pagamento, siano ridotti al minimo, è essenziale che i prestatori di servizi di pagamento siano tenuti a segnalare senza indugio i principali incidenti di sicurezza alle autorità competenti. Dovrebbe essere affidato un ruolo di coordinamento dell'ABE.*
[…]
(95) La sicurezza dei pagamenti elettronici è fondamentale per garantire la protezione degli utenti e lo sviluppo di un contesto affidabile per il commercio elettronico. Tutti i servizi di pagamento offerti elettronicamente dovrebbero essere prestati in maniera sicura, adottando tecnologie in grado di garantire l'autenticazione sicura dell'utente e di ridurre al massimo il rischio di frode. Non si ravvisa la necessità di garantire lo stesso livello di protezione per le operazioni di pagamento disposte ed eseguite con modalità diverse rispetto all'uso di piattaforme o dispositivi elettronici, ad esempio operazioni di pagamento su supporto cartaceo, ordini per corrispondenza o ordini telefonici. Una crescita robusta dei pagamenti tramite Internet e dispositivi mobili dovrebbe essere accompagnata da un potenziamento generalizzato delle misure di sicurezza. I servizi di pagamento offerti via Internet o tramite altri canali a distanza - il cui funzionamento non dipende dal luogo fisico in cui sono situati il dispositivo per disporre l'operazione di pagamento o lo strumento di pagamento - dovrebbero pertanto comportare l'autenticazione delle operazioni attraverso codici dinamici, affinché l'utente sia, in ogni momento, al corrente dell'importo e il beneficiario dell'operazione che l'utente sta autorizzando.
(96) Le misure di sicurezza dovrebbero essere compatibili con il livello di rischio insito nel servizio di pagamento prestato. Al fine di permettere lo sviluppo di mezzi di pagamento di facile uso e accessibili per pagamenti a basso rischio, come i pagamenti di importo ridotto senza contatto fisico al punto vendita, basati o meno su telefono cellulare, le esenzioni dall'applicazione dei requisiti di sicurezza dovrebbero essere specificate in norme tecniche di regolamentazione. L'uso sicuro di credenziali di sicurezza personalizzate è necessario per limitare i rischi connessi al phishing e ad altre attività fraudolente. Al riguardo, l'utente dovrebbe poter fare affidamento sull'adozione di misure che tutelano la riservatezza e l'integrità delle credenziali di sicurezza personalizzate. Tali misure comprendono di norma sistemi di cifratura basati su dispositivi personali del pagatore, tra cui lettori di carte o telefoni cellulari, o forniti al pagatore dal proprio prestatore di servizi di pagamento di radicamento del conto mediante canali diversi, come SMS o posta elettronica. Le misure, comprendenti normalmente i sistemi di cifratura, che possono dar luogo a codici di autenticazione quali password monouso, sono in grado di potenziare la sicurezza delle operazioni di pagamento. L'uso di tali codici di autenticazione da parte degli utenti dei servizi di pagamento dovrebbe essere considerato compatibile con i relativi obblighi in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate, anche quando sono coinvolti prestatori di servizi di disposizione di ordine di pagamento o prestatori di servizi di informazione sui conti.»

diligenza dell'intermediario nell'esecuzione dei contratti.

Ebbene, si può pacificamente asserire che la dottrina più risalente (nonché consolidata) abbia mostrato di individuare una responsabilità particolarmente approfondita in capo alle banche. Ciò in ragione del dibattito sorto intorno ai canoni di condotta esigibili dalle aziende di credito nell'erogazione dei loro servizi alla clientela, nel corso del quale si è giunti al punto da postulare una vera e propria "diligenza del buon banchiere"[35], istituto così caratterizzato da portare una parte della dottrina a teorizzare una vera e propria responsabilità da status[36] in capo all'intermediario[37] sulla scorta della teoria del cd. "contatto sociale", indicazione successivamente raccolta dagli Ermellini.

Infatti, quasi trent'anni fa[38] la Corte di Cassazione ha chiarito come la diligenza del *bonus argentarius* sia caratterizzata da quel maggior grado di prudenza ed attenzione che la connotazione professionale dell'agente richiede. Non solo, essa deve trovare applicazione tanto in riferimento ai contratti bancari in senso stretto quanto ad ogni tipo di atto o di operazione posta in essere, nell'esercizio della sua attività, dalla banca, la quale deve predisporre qualsiasi mezzo idoneo onde evitare il verificarsi di eventi pregiudizievoli comunque prevedibili.

Altro orientamento, invero, postula l'applicazione della disciplina prevista per il mandato e, seguendo un percorso ermeneutico strettamente aderente alla lettera della norma, è stato evidenziato come l'art. 1856 c.c. prescriva, nell'esecuzione degli incarichi bancari, di attenersi alle regole del mandato[39]. Detta norma opera un doppio richiamo, in quanto si ricollega prima al concetto di diligenza del buon padre di famiglia di cui all'art. 1710 c.c. e, per suo tramite, richiama il comma 1 dell'art. 1176 c.c.. Così facendo, però si postulerebbe un canone di condotta diverso rispetto a quello — assai più severo — della diligenza professionale, enunciata al comma 2 della medesima disposizione e alla quale va ricondotta la "diligenza del buon banchiere"[40].

Altri interpreti, ancora, hanno inquadrato l'attività in questione nell'ambito

---

[35] Dibattito, peraltro, che ha radici risalenti alla seconda metà dello scorso secolo, visto che già è affrontato in G. FERRI, *La diligenza del buon banchiere*, in *Banca borsa tit. cred.*, 1958, I, 1 e in P. VITALE, *Fondamento e limiti della "libertà" del banchiere nel pagamento degli assegni bancari*, 1959, I, 513. In giurisprudenza (cfr. Cass., 12.04.2018, n. 9158, questa con nota di M. C. DOLMETTA, *Responsabilità dell'intermediario in caso di operazioni fraudolente effettuate a mezzo di strumenti elettronici*, su www.dirittobancario.it, del 16 maggio 2018; Cass., 03.02.2017, n. 2950 con nota di L. ASTORRI, *Home banking: responsabilità del prestatore dei servizi di pagamento per operazioni disposte da terzi*, su www.dirittobancario.it, del 1° marzo 2017; Cass., 19.01.2016, n. 806 su http://www.italgiure.giustizia.it/sncass/; Cass., 12.06.2007, n. 13777 su https://plusplus24diritto.ilsole24ore.com/; Coll. Coord., 12.06.2019, n. 14447 su https://www.arbitrobancariofinanziario.it/decisioni/index.html) si parla della figura dell'*accorto banchiere*, che va ritenuta identica a quella teorizzata in dottrina.

[36] C. SCOGNAMIGLIO, *Sulla responsabilità dell'impresa bancaria per violazione di obblighi discendenti dal proprio status*, in *Giur. it.*, 1995, I, 1, 356; *Id., Ancora sulla responsabilità della banca per violazione di obblighi discendenti dal proprio status*, in *Banca borsa tit. cred.*, 1997, II, 655; N. MARZONA, *Lo status (professionalità e responsabilità) della banca in una recente sentenza della Cassazione*, 1994, II, 266.

[37] Tale responsabilità da *status* potrebbe benissimo ricollegarsi, poi, alla necessità che l'intermediario si accolli interamente il cd. "rischio di impresa" delineato in accorta dottrina e recentemente accolto nella giurisprudenza arbitrale di cui si dirà nel prossimo paragrafo (cfr. Coll. Coord., 26.07.2018, n. 16237 https://www.arbitrobancariofinanziario.it/decisioni/index.html; Coll. Coord., 26.10.2012, n. 3498 su https://www.arbitrobancariofinanziario.it/decisioni/index.html; Coll. Roma, 15.10.2010, n. 1111 su https://www.arbitrobancariofinanziario.it/decisioni/index.html)

[38] Cass., 07.05.1992, n. 5421 su https://plusplus24diritto.ilsole24ore.com/

[39] Cass., 18.03.2010, n. 6624 su https://plusplus24diritto.ilsole24ore.com/

[40] In questo senso vedasi Cass., 12.05.2021, n. 12573 su http://www.italgiure.giustizia.it/sncass/

della responsabilità da trattamento dei dati ai sensi dell'art. 31, d.lgs. n. 196/2003, con la conseguenza che veniva altresì considerato il rinvio operato dall'art. 15, d.lgs. n. 196/2003 al regime delle attività pericolose ex art. 2050 c.c.[41].

2.2 La novella *post* PSD2 e l'operato dell'Arbitro Bancario Finanziario.

Tali impostazioni ermeneutiche sono state, poi, arricchite in seguito alle novità introdotte dalla Direttiva PSD2, nonché dalla maggior rilevanza acquisita da un ulteriore *player*, l'Arbitro Bancario Finanziario[42].

Attore che, oltre ad aver accolto quell'impostazione basata sulla responsabilità professionale qualificata[43] – ex art. 1176, co. 2, c.c. – ha fatto propria anche quella giurisprudenza di legittimità che, con specifico riferimento ai servizi e strumenti che si avvalgono di mezzi meccanici o elettronici (compresi i servizi di pagamento), ha chiarito come l'istituto bancario non possa non adottare misure idonee a garantire la sicurezza del servizio stesso, attesa la natura tecnica della diligenza posta a suo carico, da valutarsi tenendo conto dei rischi tipici della sfera professionale di riferimento[44].

Tuttavia, va precisato come l'operato ermeneutico dell'Arbitro sia differente in quanto, da un lato è giunto a postulare persino un dovere di monitoraggio delle operazioni di pagamento svolte dai propri utenti e a ricomprenderla nel perimetro della diligenza del buon banchiere[45] mentre, dall'altro lato, richiama

[41] Trib. Palermo, 12.01.2010, n. 81 su https://plusplus24diritto.ilsole24ore.com/, recentemente ripresa in Cass., 12.04.2018, n. 9158 su http://www.italgiure.giustizia.it/sncass/. Nello stesso senso ma con considerazioni pure sull'operatività del disposto ex art. 1176 c.c. vedasi Trib. Siracusa, 15 marzo 2012 su https://plusplus24diritto.ilsole24ore.com/

[42] Vero è che l'Arbitro Bancario Finanziario (ABF) è stato istituito nel 2009 in attuazione dell'articolo 128-*bis* del Testo unico bancario (TUB), introdotto dalla legge sul risparmio (legge n. 262/2005). Ma è pure vero che ha acquisito rilevanza solo con il trascorrere del tempo, iniziando con un "carico" di 3.409 ricorsi presentati nel primo anno di operatività (cfr. BANCA D'ITALIA (a cura della), *Relazione sull'attività dell'Arbitro Bancario Finanziario*, n. 1, 2010) per arrivare ai 13.575 ricorsi del 2015 e ai 30.918 ricorsi nel 2020 (vedasi la *Relazione sull'attività dell'Arbitro Bancario Finanziario* del 2015 e la si confronti anche con quella del 2020).

[43] Cfr. Coll. Coord., 26.10.2012, n. 3498, che richiama anche Coll. Roma, 15.10.2010, n. 1111, entrambe su https://www.arbitrobancariofinanziario.it/decisioni/index.html. Nello stesso senso Coll. Roma, 17.06. 2010, n. 544 e Coll. Napoli, 10.09.2019, n. 21064 – Rel. GATT, su https://www.arbitrobancariofinanziario.it/decisioni/index.html

[44] Cass., 12.06.2007 n. 13777, su https://plusplus24diritto.ilsole24ore.com/; nello stesso senso anche Cass., 24.09.2009, n. 20543 su https://plusplus24diritto.ilsole24ore.com/, mentre per la giurisprudenza merito vedasi Trib. Parma, 06.09.2018, n. 1268 su https://plusplus24diritto.ilsole24ore.com/, Trib. Verona, 02.10. 2012 su https://plusplus24diritto.ilsole24ore.com/.

[45] Coll. Napoli, 14.01.2013, n. 311 su https://www.arbitrobancariofinanziario.it/decisioni/index.html; vedasi anche Coll. Napoli, 28.11.2018, n. 25152 – Rel. GATT su https://www.arbitrobancariofinanziario.it/decisioni/index.html, dove è stigmatizzata la condotta dell'intermediario per aver mancato in una attività che rientra chiaramente nel monitoraggio delle operazioni degli utenti, in quanto «*Nel caso di specie il Collegio, pur ritenendo sussistere detta serie univoca e concordante di elementi atti a dimostrare un contegno colposo da parte del ricorrente - in ragione del fatto che le operazioni sono avvenute a non rilevante distanza di tempo dal furto dello strumento di pagamento - circostanza che lascia presumere la conservazione dei codici PIN unitamente alla carta stessa (Coll. Napoli, n. 11185/2016) – non può non rilevare altresì l'allegazione di 13 tentativi non andati a buon fine, nell'arco della medesima giornata e a distanza ravvicinata l'uno dall'altro. Elemento questo che induce a ritenere anche l'intermediario corresponsabile dell'evento dannoso ai sensi dell'art. 1227 c.c. Peraltro, anche la circostanza che i sette prelievi disconosciuti si siano susseguiti tra le 11:58 e le 12:59, vale a dire nell'arco temporale di circa un'ora nel medesimo giorno, rappresenta un elemento idoneo a distribuire parte della responsabilità alla negligenza dell'intermediario.*». All'interno dell'obbligo di monitoraggio (ma con più stretta connessione alla corretta esecuzione del contratto) si può ricondurre anche l'ipotesi dell'intermediario che consenta un uso della carta oltre i limiti di importo pattuiti (Coll. Napoli, 14.05.2019, n. 12125 – Rel. GATT su

ampiamente la disciplina settoriale predisposta con il d.lgs. n. 11/2010.

Per cui, se la giurisprudenza ordinaria tende ad applicare le norme codicistiche, i Collegi arbitrali fondano le loro decisioni soprattutto sul disposto del d.lgs. n. 11/2010 e sviluppano gli orientamenti già affrontati dai loro "colleghi" magistrati.

Anzi, si può ben dire che i membri dei Collegi arbitrali affrontino con maggior severità i casi di lamentata negligenza in capo ai *provider* di servizi di pagamento.

Infatti, se applicando i parametri della responsabilità professionale ex artt. 1176, co. 2 e 2050 c.c., si giunge a chiedere all'intermediario una prova liberatoria particolarmente approfondita, si ha comunque un regime differente rispetto a quello delineato dagli artt. 10, 11 e 12, d.lgs. n. 11/2010, i quali, tra l'altro, paiono configurare una fattispecie di responsabilità oggettiva frequente in ambito bancario[46], che caratterizza proprio gli orientamenti della giurisprudenza arbitrale[47].

È così che se la prova richiesta in tema di responsabilità professionale attiene alla dimostrazione di aver adottato tutte le misure necessarie e idonee a qualificare concretamente la propria diligenza come rientrante nell'art. 1176, co. 2, c.c., a questa si aggiunge la necessità di provare, alternativamente, la colpa grave, il dolo ovvero l'intento fraudolento del titolare dello strumento di

---

https://www.arbitrobancariofinanziario.it/decisioni/index.html), in quanto per potersi avere un "blocco" di simili operazioni è necessario monitorare le stesse.

[46] M. C. Paglietti, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, in *Innovazione e regole nei pagamenti digitali – Il bilanciamento degli interessi nella PSD2*, a cura di M. C. Paglietti e M. I. Vangelisti, Roma TrE-PRESS, 2020, p. 49, dove si legge «*Il tema del criterio d'imputazione della responsabilità, declinato secondo la retorica dell'individuazione del soggetto su cui più efficientemente far ricadere il danno (colui sul quale, cioè, coesianamente, far gravare il costo degli incidenti), è il cuore delle disposizioni e delle scelte politiche in materia, che, nei vari ordinamenti, propongono un'allocazione articolata delle perdite subìte, risentendo della maggiore propensione ad optare per la soluzione della responsabilità oggettiva limitata laddove l'attività bancaria venga ascritta alle attività pericolose.*»

[47] Posizione, tra l'altro, che trova numerosi echi anche nella giurisprudenza di legittimità in tema di contratti bancari, tant'è vero che, per esempio, in Cass., 19.07.2012, n. 12448 su https://plusplus24diritto.ilsole24ore.com/, il collegio giudicante si esprime nei seguenti termini testuali (richiamando numerose pronunce): «*A norma dell'art. 2049, la società di intermediazione è responsabile degli illeciti commessi dal promotore finanziario anche a titolo oggettivo, cioè indipendentemente da comportamenti negligenti o colposi suoi propri, in relazione ai danni che l'investitore possa avere subito per avere fatto affidamento sull'esistenza del rapporto di preposizione. Ciò in considerazione dei rischi inerenti all'esercizio di attività finanziarie e delle gravi perdite a cui gli eventuali illeciti degli addetti possono esporre la clientela: rischi che la società di intermediazione è in grado di gestire, e danni contro i quali ha la possibilità di premunirsi (anche tramite l'assicurazione), in termini più efficaci, più razionali e meno costosi, che non il singolo investitore. Trattasi dei noti principi da tempo elaborati dalla dottrina in tema di responsabilità per rischio di impresa, che nell'ambito delle attività finanziarie trovano particolari ragioni per essere riaffermati, e che in questo campo la giurisprudenza di legittimità ha effettivamente ribadito con rigore (cfr., proprio con riferimento ad un caso di indebita appropriazione del denaro dei clienti da parte del promotore finanziario, Cass. civ. Sez. 1, 24 luglio 2009 n. 17393: "Sussiste la responsabilità indiretta della banca nei confronti dei terzi per il comportamento illecito del promotore finanziario allorché, indipendentemente dall'esistenza di un rapporto di lavoro subordinato e dal carattere di continuità dell'incarico, l'attività del promotore sia stata agevolata o resa possibile dal suo inserimento nell'attività d'impresa (dalla sua presenza nella sede, dall'utilizzo della modulistica di pertinenza, dalla spendita del nome, ecc.), e sia stata realizzata nell'ambito e coerentemente alle finalità in vista delle quali l'incarico è stato conferito, in maniera tale da far apparire 8 al terzo in buona fede che l'attività posta in essere per la consumazione dell'illecito rientrasse nell'ambito dell'incarico affidato dalla mandante". Vedi anche, fra le tante, Cass. civ. Sez. 1, 22 ottobre 2010 n. 21729; Cass. civ. Sez. 3, 25 gennaio 2011 n. 1741, che ha ravvisato la responsabilità in un caso in cui il promotore aveva provocato il danno svolgendo attività in conflitto di interessi con la società mandante, cioè vendendo i prodotti di altra società, per il solo fatto che l'illecito è stato compiuto nel quadro delle attività funzionali all'esercizio delle incombenze affidate al promotore. Per un caso analogo, con riferimento alla L. n. 1 del 1991, art. 5, Cass. civ. Sez. 3, 19 luglio 2002 n. 10580).*»

pagamento[48] nell'ottica di una esclusione della propria responsabilità di tipo oggettivo.

E, invero, tale è l'unica conclusione cui si può giungere in tema di riparto dell'onere probatorio, giusto il disposto dell'art. 10, d.lgs. n. 11/2010, rubricato "*Prova di autenticazione ed esecuzione delle operazioni di pagamento*"[49], dove si prevede al comma 1 un onere probatorio ben inquadrabile nel solco della diligenza ex art. 1176, co. 2 c.c., cui si *aggiunge*, però, quello relativo alla prova della frode, del dolo o della colpa grave in capo all'utente disposto al comma 2, a chiusura della disposizione.

Per cui, è oramai pacifico come l'intermediario sia chiamato a provare tanto la propria diligenza quanto, almeno, la colpa grave dell'utente, dovendosi raggiungere entrambe le prove ai fini di una esclusione della propria responsabilità.

Tuttavia, nella consapevolezza che così procedendo si rischia di prospettare una quasi sistematica responsabilità del *provider* che fornisce il servizio di *home banking*, i Collegi territoriali[50] hanno evidenziato l'importanza di una analisi approfondita delle circostanze del singolo caso al fine di vagliare attentamente possibili profili di negligenza dell'utente[51].

Pertanto, se può sostenersi la netta responsabilità del *provider* che trascuri l'adozione dei più avanzati accorgimenti tecnici di prevenzione in spregio all'obbligo di diligenza[52], la medesima responsabilità potrebbe essere esclusa, in tutto o quantomeno in parte, nell'ipotesi in cui il cliente, debitamente informato circa l'aggiornamento dei presidi di sicurezza (quale è, per esempio, un sistema di generazione e invio di codici *One Time Password*), ometta di avvalersene, venendo meno ai propri personali obblighi di custodia.

---

[48] In tal senso, successivamente alla novella del d.lgs. n. 11/2010, va chiarito come vi sia una vera e propria unanimità nella giurisprudenza degli Ermellini e in quella dell'ABF (cfr. Cass., 26.05.2020, n. 9721, con nota di G. SPATARO, *Bancomat: prelievi abusivi da parte di terzi e riparto di responsabilità tra banca e correntista*, su www.dirittobancario.it, del 13 ottobre 2020; Cass., 03.02.2017, n. 2950 su http://www.italgiure.giustizia.it/sncass/; Coll. Coord., 26.10.2012 n. 3498, *cit.*), pur permanendo un maggior ricorso dell'ABF ai suddetti dati normativi.

[49] « *1. Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.*

1-bis. Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, questi ha l'onere di provare che, nell'ambito delle proprie competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti connessi al servizio di disposizione di ordine di pagamento prestato.

2. Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente.»

[50] Coll. Milano, 25.07.2012, n. 2594 e Coll. Napoli, 03.04.2013, n. 1802 su https://www.arbitrobancariofinanziario.it/decisioni/index.html.

[51] Per esempio, in Coll. Napoli, 15.05.2019 n. 12269 – Rel. GATT su https://www.arbitrobancariofinanziario.it/decisioni/index.html è stata affrontata una ipotesi di *phone hijacking*, dove si è avuto il rigetto del ricorso per carenza probatoria da parte della ricorrente, la quale non ha dimostrato la presenza di un *man in the middle*

[52] Coll. Napoli., 05.11.2019 n. 24101 su https://www.arbitrobancariofinanziario.it/decisioni/index.html

E, proprio in tal senso, gli Arbitri hanno dato vita a differenti filoni interpretativi in merito alla valutazione della condotta dell'utente, che qui non saranno illustrati[53].

3. La sostanziale inefficacia del sistema di tutele.

Come si è visto, la *ratio* complessiva della normativa settoriale in tema di strumenti di pagamento e di operazioni di acquisto su base elettronica è basata su due elementi principali[54]:

- favorire la diffusione di tali modalità di pagamento alternative al classico contante fornendo la massima sicurezza dei sistemi informatici;
- ottenere la fiducia degli utenti.

Ciononostante, tale obiettivo è perseguito operando un bilanciamento di interessi molto particolare, caratterizzato soprattutto dalla previsione di obblighi e responsabilità che, alla prova dei fatti, ricadono quasi unicamente sugli intermediari, sbilanciando l'impianto normativo stesso a favore del consumatore, tradizionalmente considerato la parte debole nei rapporti contrattuali di tipo *business to consumer* (B2C).

Tale sbilanciamento, tra l'altro, è alquanto "rafforzato" dalla giurisprudenza predominante in materia di contratti bancari e preesistente rispetto alle ultime novelle operate nei confronti del d.lgs. n. 11/2010.

Però, non può dirsi che una simile disciplina, così *astrattamente* favorevole verso l'utente dei servizi di pagamento, abbia sortito l'effetto sperato, dal momento che la fiducia dei consumatori negli strumenti di pagamento elettronici è effettivamente aumentata in tempi recenti, ma certamente non in conseguenza delle larghe tutele previste per gli stessi all'interno del d.lgs. n. 11/2010, quanto, piuttosto, in considerazione dei vantaggi derivanti dal cd. "*cashback* di Stato" avviato nell'ambito del "*Piano Italia Cashless*", previsto dalla Legge di Bilancio 2020 (art. 1, co. 288 - 290, l. n. 160/2019) e dal Decreto del Ministero dell'Economia e delle Finanze n. 156 del 24 novembre 2020, unitamente alle esigenze derivanti dal distanziamento sociale disposto a causa della pandemia.

---

[53] Comunque, valga quanto segue ai fini di un approfondimento. Alcuni degli orientamenti risultano essere quali più rispondenti alla *ratio* e alla lettera della norma e tendenti all'esclusione di automatismi in sede probatoria che ribaltino il rapporto di *favor* previsto dalla norma per il titolare dello strumento di pagamento (cfr. Coll. Napoli, 08.10.2012 n. 3192 su https://www.arbitrobancariofinanziario.it/decisioni/index.html, che si esprime nei seguenti termini: «*gli orientamenti di questo Collegio sono nel senso che "l'adozione da parte dell'intermediario di valide ed efficaci misure di tutela degli interessi dell'utilizzatore, se non può ritenersi valere ad escludere senz'altro la sua responsabilità e, di riflesso, a dimostrare che l'intromissione fraudolenta nel sistema di protezione da lui predisposta sia imputabile alla grave (in rapporto alla massima sicurezza offerta dall'intermediario) negligenza o imprudenza dell'utilizzatore (per non avere custodito adeguatamente le proprie credenziali: art. 12, n. 4), vale sicuramente ad elevare in modo significativo il livello delle allegazioni richieste al cliente, al fine di rendere adeguatamente verosimigliante il carattere fraudolento dell'operazione" (così nella decisione n. 1334/1912), venendo, in difetto, altrimenti sancito – a fronte di soluzioni tecnologicamente avanzate – una inammissibile sottrazione del prestatore dei servizi di pagamento a ogni forma di responsabilità*». In senso conforme all'orientamento degli arbitri partenopei si veda anche il Collegio di Roma con varie decisioni (*ex multis*, 28.06.2012, n. 2264, nonché 30.07.2012, n. 2660) e altri di senso opposto (vedasi Coll. Milano, 17.02.2012 n. 528, di recente superato per accogliere l'impostazione del Collegio di Napoli), tutti su https://www.arbitrobancariofinanziario.it/decisioni/index.html

[54] M. C. Paglietti, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, *cit.*, p. 44

Al tempo stesso, non solo le disposizioni del d.lgs. n. 11/2010 non sembrano garantire adeguate tutele effettive all'utente del servizio di pagamento – ciò in quanto una cosa è ottenere un rimborso, magari parziale, del danaro trafugato e ben altra cosa è usufruire di un sistema che riconosce e blocca efficacemente le frodi impedendole *in toto* – ma, in ragione dei tempi comunque relativamente (e fisiologicamente) lunghi per far valere le proprie ragioni, ad esempio in sede arbitrale (generalmente previo reclamo al proprio *provider*), l'impianto complessivo delle tutele risulta inadeguato a perseguire il fine di ottenere la *fiducia* dell'utente stesso[55].

Poi, siffatta modalità di pagamento ovviamente non incontra, lato tutele, il favore degli intermediari per gli oneri probatori che pone in capo agli stessi per dimostrare di aver adempiuto ai propri obblighi di diligenza "bancaria" ma, soprattutto, è osteggiata dagli stessi esercenti (tanto dei negozi fisici che degli *store online*) per via degli *step* di autenticazione che richiede per limitare il rischio di transazioni non autorizzate[56], che rendono farraginose le operazioni di pagamento.

Ne consegue la necessità di riflettere e verificare se non sia il caso, piuttosto, di spostare il *focus* complessivo, dagli strumenti di tutela ordinari previsti per il titolare dello strumento di pagamento a un ripensamento dell'architettura internazionale (e interna, dal momento che sono similari) dei sistemi di pagamento digitali in sé (in considerazione del fatto che buona parte dei fondi distratti dai conti correnti italiani vengono dirottati in altri Paesi).

Infatti, è oramai pacifico che, pur attuando tutte le tutele volte a prevenire le frodi e pur ponendo un obbligo di rimborso a carico dei *provider*, comunque queste non sono scelte idonee a ridurre concretamente il rischio di operazioni non riconosciute derivante dalla diffusione di strumenti di pagamento digitali, le quali stanno, anzi, aumentando.

Ciò in quanto, da un lato corrisponde al vero che sono migliorate le modalità di autenticazione dell'utente ma, dall'altro, è pur vero che l'architettura di sistema su cui "viaggiano" le transazioni è complessivamente rimasta la medesima dalla seconda metà dello scorso secolo[57], senza che si siano avuti aggiornamenti sufficientemente radicali da rendere obsolete numerose modalità di captazione dei dati di accesso le quali, *de facto*, sono rimaste le stesse.

---

[55] Per esempio, in un caso seguito dal Collegio di Napoli (Coll. Napoli, 25.03.2021 n. 8323, su https://www.arbitrobancariofinanziario.it/decisioni/index.html) la frode si è verificata il 18 febbraio 2020 e, tra reclamo all'intermediario, presentazione del ricorso, calendarizzazione e adunanza del Collegio, la decisione – di rigetto del ricorso, tra l'altro – è arrivata più di un anno dopo. Tempi parimenti lunghi si possono riscontrare in altri Collegi. Vedasi Coll. Milano, 01.03.2021 n. 5357 su https://www.arbitrobancariofinanziario.it/decisioni/index.html, dove non risulta, dalla lettura della decisione, che vi sia stata una previa interlocuzione tra utente e intermediario e comunque ci sono voluti diversi mesi per arrivare a una decisione. Tempi pari a quelli del Collegio partenopeo (ossia un anno circa a partire dalla data della frode) si hanno anche in quello capitolino in presenza di un previo reclamo al proprio intermediario, come si evince da Coll. Roma, 01.03.2021 n. 5436 su https://www.arbitrobancariofinanziario.it/decisioni/index.html.

[56] A. S., *E-commerce, transazioni più sicure grazie all'analisi in real time*, *su www.pagamentidigitali.it/ecommerce/e-commerce-transazioni-piu-sicure-grazie-allanalisi-in-real-time/#:~:text=Grazie%20ad%20%22Advice%22%2C%20il,frodi%20con%20%22Guaranteed%20Payments%22;* .

[57] Il sistema *SWIFT* per le transazioni internazionali è nato nel corso degli anni Settanta ad opera della Society for Worldwide Interbank Financial Telecommunication

3.1. Le statistiche sull'andamento delle transazioni fraudolente.

Infatti, ponendo ora l'attenzione sulle dimensioni del fenomeno stesso – ci si riporta a un report annualmente prodotto dalla Nilson Report[58], rivista specializzata nell'ambito dei sistemi di pagamento – si nota quanto sia vasto lo stesso. Infatti, le frodi su carte di pagamento a livello globale per emittenti, esercenti e *acquirers*, utilizzate per acquisti o prelievi di contante, hanno raggiunto nel 2019 i 28,65 miliardi di dollari, con un aumento del 2,9% rispetto all'anno precedente, da rapportare a un volume di transazioni a mezzo pagamenti elettronici pari a oltre 42 trilioni di dollari, pure aumentato del 4,2% rispetto al 2018.

L'anno precedente, invece, le frodi su carte di pagamento a livello globale hanno avuto una crescita pari a oltre il 16% per un valore complessivo di 27,85 miliardi di dollari, rapportata a un totale di transazioni complessive pari a oltre 40 trilioni di dollari, in aumento del 17,7% rispetto al 2017[59].

Quindi, l'incidenza complessiva delle frodi, espressa in termini percentuali rispetto al totale delle operazioni svolte, è costantemente in diminuzione, come si evince dai dati illustrati nella tabella qui allegata (vedasi la figura che segue – terza colonna verso destra). Ciononostante, secondo le proiezioni statistiche si prevede una recrudescenza delle stesse frodi proprio in questi due anni caratterizzati dalla pandemia.

Card Fraud Projected Worldwide

YEAR	Total Volume TRILLIONS	Fraud BILLIONS	Cents per $100 VOLUME
2015	$31.310	$21.84	6.97¢
2016	$31.878	$22.80	7.15¢
2017	$34.472	$23.97	6.95¢
2018	$40.582	$27.85	6.86¢
2019	$42.274	$28.65	6.78¢
2020	$42.241	$30.93	7.32¢
2021	$44.829	$32.04	7.14¢
2022	$47.627	$31.52	6.62¢
2023	$50.375	$32.96	6.54¢
2024	$53.245	$34.40	6.46¢
2025	$56.182	$35.31	6.28¢
2026	$59.284	$36.93	6.23¢
2027	$62.614	$38.50	6.15¢
2028	$66.188	$40.05	6.05¢

© 2020 Nilson Report

60

Variazione del valore delle frodi con sistemi di pagamento elettronici nel mondo rapportato al valore complessivo delle transazioni.

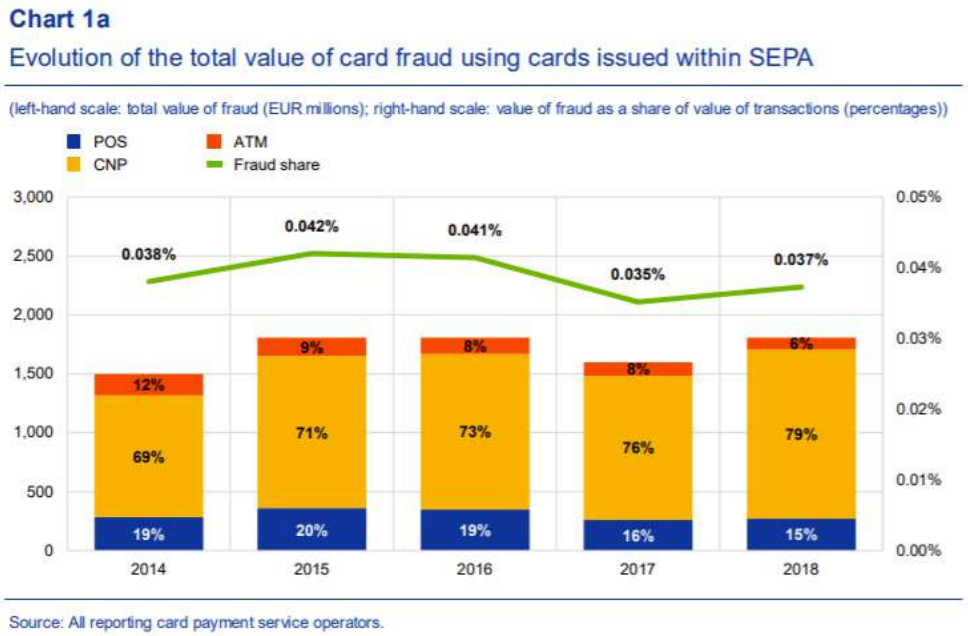
[58] REDAZIONE, *Card Fraud Losses Worldwide*, in *Nilson Report*, n. 1187 del dicembre 2020, disponibile gratuitamente al link https://nilsonreport.com/content_promo.php?id_promo=16

[59] REDAZIONE, *Card Fraud Losses Reach $27.85 Billion*, in *Nilson Report*, n. 1164 del novembre 2019, disponibile gratuitamente al link https://nilsonreport.com/mention/407/1link/#

[60] REDAZIONE, *Card Fraud Losses Worldwide*, cit., p. 5

Concentrando lo sguardo sull'area SEPA, poi, si rinviene un similare trend di crescita delle frodi, forse anche più pronunciato, anche se i dati statistici analizzati nel *Sixth report on card fraud* della BCE sono limitati al 2018.

Per la precisione, se le transazioni totali hanno quasi raggiunto il valore di 5 trilioni di euro nel 2018 con una crescita del 6,5% rispetto al 2017, si è registrato un aumento assai più rilevante delle frodi, tanto in termini di valore assoluto (1,8 miliardi di euro) che in termini percentuali rispetto all'anno precedente (+13%), con una incidenza delle transazioni fraudolente sul totale che è tornata a crescere.



61

Variazione del valore delle frodi con sistemi di pagamento elettronici nell'area SEPA con indicazione dell'incidenza sul totale delle transazioni.

3.2 Una possibile evoluzione dei sistemi di pagamento attraverso IA e *blockchain.*

Da quanto finora delineato, si comprende come sia necessario intervenire a monte, ossia sull'architettura tecnica del sistema di pagamento, per poi modificare e adeguare anche il relativo substrato di previsioni giuridiche.

Una prima ipotesi di innovazione sarebbe l'applicazione della *blockchain* all'ambito dei sistemi di pagamento elettronici (che pure è il suo "ambiente" naturale, visto che è nata come mezzo di scambio delle criptovalute [62]), soluzione che pare già tenuta in considerazione, tant'è vero che in una pubblicazione molto lungimirante della Cassa Depositi e Prestiti si analizza

[61] BCE, *Sixth report on card fraud*, 2020, p. 8, disponibile al link https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202008~521edb602b.en.pdf

[62] S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponibile al link https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf. Si noti che il nome dell'autore è uno pseudonimo che nasconde l'inventore della criptovaluta Bitcoin

proprio l'attuale sistema di pagamenti *cross border* basato su SWIFT[63] e si ipotizza la sua sostituzione con un sistema completamente nuovo, su base *blockchain*, che prevede perfino l'utilizzo di *digital asset* ai fini della gestione dei pagamenti stessi, in modo da rendere più certe e celeri le transazioni transfrontaliere operate da Piccole e Medie Imprese.

Ora, laddove dovesse essere sperimentata con successo nell'ambito della PMI, una architettura informatica simile ben si presterebbe ad essere adeguata e applicata su scala ben più vasta, ossia a livello *retail*[64], anche per assolvere non solo al monitoraggio antifrode ma anche per garantire il corretto funzionamento del sistema contro ipotesi quali quella del *double spending*[65].

La tecnologia a "registri distribuiti", tuttavia, non sarebbe idonea da sola a porre un freno alle transazioni fraudolente, laddove i sistemi di *autenticazione* degli utenti e quelli di *monitoraggio* delle operazioni dovessero rimanere sostanzialmente gli stessi.

E, invero, se l'autenticazione biometrica è già prevista, non può dirsi lo stesso per l'utilizzo di Intelligenze Artificiali quali sistemi di monitoraggio.

Anzi, potrebbe affermarsi che vi sia un divieto di essere sottoposti a decisioni automatizzate[66], la cui *ratio* è quella di garantire in ogni momento la possibilità di ottenere la modifica ovvero la disattivazione degli algoritmi impiegati in tal senso.

Tuttavia, sussistono delle eccezioni a tale divieto:

- l'ipotesi che l'utilizzo dell'IA sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- l'utilizzo dell'IA sia autorizzato a livello europeo o nazionale, fatti salvi i diritti e le libertà fondamentali;
- l'utilizzo dell'IA sia fondato sul consenso dell'interessato.

Ebbene, per quanto concerne il caso del monitoraggio delle transazioni di un individuo (che già avviene, per la verità), va detto che anche ora, senza alcuna modifica normativa da effettuarsi, potrebbero sussistere, cumulativamente, i presupposti per l'applicazione delle IA al monitoraggio bancario.

---

[63] CDP-SIA-IBM, *Ipotesi di adozione della tecnologia blockchain in ambito finanziario*, su *www.cdp.it/resources/cms/documents/White_paper_tecnologia_blockchain_CDP_SIA_IBM.pdf*, p. 36 ss.

[64] Un progetto più *retail* è perseguito proprio a livello nazionale con il progetto *Spunta* di ABILab (link https://www.abilab.it/aree-ricerca/blockchain-dlt/spunta-banca-dlt), finalizzato a gestire i conti interbancari con una tecnologia *blockchain* condivisa in luogo della precedente, basata su registri bilaterali

[65] M. F. MONTEROSSI, *Intelligenza artificiale e blockchain: implicazioni reciproche*, in I*ntelligenza artificiale e diritto – come regolare un mondo nuovo*, a cura di A. D'ALOIA, Franco Angeli S.r.l., 2020, p. 480

[66] Cfr. Art. 22 GDPR – «*1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*
2. Il paragrafo 1 non si applica nel caso in cui la decisione:
a)sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b)sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.»

Infatti, è chiaro che ricorrerebbe la prima eccezione, dal momento che tutti i contratti bancari fanno espresso riferimento al trattamento dei dati ai fini dell'esecuzione degli stessi.

Parimenti, essendovi una normativa che consente il trattamento dei dati dell'utente ai fini della prevenzione delle frodi, si rientrerebbe nel campo di applicazione della seconda eccezione[67].

In ultimo, sarebbe possibile soddisfare anche l'ultima eccezione in considerazione del fatto che, in sede di stipula dei contratti bancari, è oramai richiesto il consenso dell'interessato al fine del trattamento dei suoi dati[68].

Così ragionando e ricomprendendo il monitoraggio a mezzo IA nell'ambito del concetto di "trattamento automatizzato", è possibile ipotizzare che già a legislazione vigente si possano adottare le Intelligenze Artificiali nei processi di monitoraggio interno delle banche.

Rimane comunque, in una ottica *de iure condendo*, la necessità di adottare una apposita normativa, quantomeno a livello europeo, per regolamentare l'uso dell'IA in ambito bancario, non potendocisi affidare unicamente a un procedimento di ermeneusi, stante la sua inadeguatezza a fornire contorni più certi a scenari attualmente molto sfumati[69], con tutti i rischi del caso.

Tale necessità diventa ancor più impellente se si considerano i profili inerenti tanto alla soggettività giuridica di simili sistemi automatizzati quanto all'etica stessa, dovendosi *progettare* sistemi automatizzati così evoluti da soddisfare la necessità di un comportamento etico delle macchine.

Anzi, nel corso di una intervista alla Prof.ssa Gatt [70] quale direttore del *Research Centre of European Private Law* (ReCEPL) per la rivista Diritto Mercato Tecnologia[71], alla domanda su quali possano essere i rischi di un

---

[67] Art. 29, d.lgs. n. 11/2010 - «*1. I prestatori di servizi di pagamento e i gestori di sistemi di pagamento possono trattare dati personali ove ciò sia necessario a prevenire, individuare e indagare casi di frode nei pagamenti. La fornitura di informazioni a persone fisiche in merito al trattamento dei dati personali e ad altro trattamento ai fini del presente decreto avviene in conformità al decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.*
1-bis. I prestatori di servizi di pagamento hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei propri servizi solo previo consenso esplicito dell'utente dei servizi di pagamento.»

[68] Vedasi, ad esempio, il contratto della Fineco Bank sopra descritto in relazione agli obblighi dell'utente, il quale è tenuto a prendere visione dell'Allegato A (informativa privacy) e a fornire il relativo consenso. Ovviamente, si rende necessaria una corretta informazione dello stesso, come si ribadisce in M. F. MONTEROSSI, *Intelligenza artificiale e blockchain: implicazioni reciproche*, *cit.*, p. 485

[69] Infatti, si consideri quanto dice E. TROISI (cfr. *AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla 'intellegibilità' dell'algoritmo*, in *European Journal of Privacy Law & Technologies*, Giappichelli, *issue* 1/2019) laddove scrive che «*L'ADM è ammesso solo in presenza di quelle condizioni autorizzative per così dire "consensuali", idonee ad assicurare una più ampia consapevolezza dell'interessato, con la conseguenza che deve ritenersi illegittimo in tutti i casi in cui l'interessato non vi abbia acconsentito espressamente attraverso una propria consapevole manifestazione di volontà, o direttamente[1], o nell'ambito di un più complesso rapporto contrattuale, sul presupposto però, in quest'ultimo caso, che il trattamento automatizzato sia da considerarsi necessario[2] alla conclusione o all'esecuzione dell'accordo.*». Il problema è proprio capire *quando* ricorrano chiaramente le eccezioni previste dall'art. 29 GDPR, specialmente con riferimento a tecnologie *disruptive* come l'utilizzo della IA, a prescindere dal fatto che sia unita o meno ad altre tecnologie quali la *blockchain.*

[70] Docente ordinario presso l'Università Suor Orsola Benincasa di Napoli e titolare della Cattedra in Diritto delle Nuove Tecnologie

[71] REDAZIONE, *Per un'Intelligenza Artificiale antropocentrica. Intervista a Lucilla Gatt*, 21 febbraio 2020, su www.dimt.it; nello stesso senso vedasi L. AULINO, *Intelligenza artificiale e giustizia tra nuove soggettività giuridiche e nuove problematiche etiche e deontologiche*, in I*ntelligenza artificiale e diritto – come regolare un mondo nuovo*, a cura di A. D'ALOIA, Franco Angeli S.r.l., 2020, p. 229 ss. dove affronta la questione etica in relazione al comparto dell'amministrazione della giustizia. Ciononostante, trattasi di principi generali applicabili astrattamente a qualsiasi ambito la IA si trovi ad operare, ivi compreso anche quello bancario e della prevenzione delle frodi.

approccio normativo che non tenga conto dell'utente umano e dell'etica, si è avuta la seguente risposta:

«*Questa recente esortazione del Parlamento europeo alla Commissione si pone in linea di continuità con almeno due risoluzioni del Parlamento medesimo, adottate l'una nel febbraio 2017 e l'altra nel febbraio 2019 dal titolo "European industrial policy on artificial intelligence and robotics". Già da tempo, infatti, il Parlamento sollecita la Commissione ad emanare regole mandatory in materia di AI. Allo stato, tuttavia, la Commissione, pur non ignorando affatto il tema dell'AI, non ha accolto completamente le indicazioni del Parlamento. Ha emanato, infatti, due comunicazioni in materia di AI nel 2018 e nel 2019. Quest'ultima si intitola "Building Trust in Human-Centric Artificial Intelligent" e si accompagna a due rilevanti atti non vincolanti della Commissione o, più esattamente, dell'High-Level Expert Group on AI (AI HLEG) costituito dalla Commissione medesima nel giugno del 2018. L' AI HLEG ha elaborato e pubblicato on line due deliverables denominati "Ethics Guidelines for Trustworthy AI" dell'aprile 2019 e "Policy and Ivestment Reccomendatios for Trustworthy AI" del giugno 2019. Si vede, dunque, come entrambi gli organi europei, e la Commissione in particolare, siano profondamente consapevoli della necessità di realizzare un quadro di regole per lo sviluppo di una AI antropocentrica nel senso di tutelante e potenziante l'essere umano in quanto tale. Questa consapevolezza, però, ha finora condotto verso l'elaborazione di raccomandazioni, comunicazioni, linee giuda che, tra l'altro, si focalizzano sull'esigenza di fare delle scelte etiche e, tralasciano, comunque, in maniera più o meno evidente, di formulare regole a carattere cogente provviste di sanzione.*»

Conclusioni.

Stante il panorama in rapido rinnovamento, specialmente dal lato dell'innovazione tecnologica, si pone la questione dell'aggiornamento delle disposizioni normative.

Per ironia della sorte, proprio la corrente disciplina già è stata il prodotto di un "inseguimento" della tecnologia in sé e ugualmente pare non aver sortito effetti.

A parere dello scrivente, forse, l'errore – o, meglio, l'imprudenza – commessa in sede di stesura della PSD2 e della normativa ad essa connessa è stato quello di focalizzare l'intero comparto delle misure di sicurezza unicamente sulla fase dell'autenticazione del pagatore, trascurando il complesso delle misure di *raccolta, conservazione e analisi* dei dati delle transazioni, che ricadono in capo alle banche.

Infatti, si potrebbe quasi dire che si è posto pressoché interamente a carico dell'utente l'obbligo di tutelare in via preventiva i propri fondi, mentre le conseguenze della mancata custodia delle credenziali tendono a ricadere, per converso, sull'intermediario stesso, spesso e volentieri tacciato di mancata *vigilanza*, di mancato *monitoraggio*, di mancata *prevenzione*[72].

[72] Per tutte valga Coll. Napoli, 14.01.2013 n. 311 su https://www.arbitrobancariofinanziario.it/decisioni/index.html, dove si legge testualmente: «*La condotta dell'intermediario appare, inoltre, priva della necessaria diligenza anche con riguardo ad ulteriori e connessi obblighi derivanti dalla propria posizione contrattuale, con particolare riguardo al costante e scrupoloso*

Eppure, per come è pensato attualmente, proprio il sistema di autenticazione e di pagamento in sé non è idoneo a consentire un monitoraggio che vada oltre l'analisi basica dei dati raccolti, atteso che consente (in tal modo evitando di gravare con ulteriori costi sull'intermediario) unicamente la verifica della mera regolarità dell'accesso e della disposizione dell'ordine di pagamento. Né si potrebbe introdurre una IA a legislazione vigente e senza cambiare l'architettura dei sistemi di pagamento, giacché la base normativa è, interpretativamente parlando, troppo confusa, mentre l'attuale sistema di pagamento non è in grado di garantire una piena integrità dei dati, quantomeno non al livello della *blockchain*.

Per contro, una novella che da un lato apra all'utilizzo della *blockchain* e della IA nelle transazioni *retail*, ponendo però in contemporanea l'obbligo – per il *provider* – di adottare tali innovazioni, unitamente alla previsione di un obbligo – questo in capo al titolare di strumenti di pagamento – di utilizzo di dati biometrici per aversi una SCA adeguata a proteggere transazioni di una certa importanza (altrimenti si avrebbe una grande falla nel sistema di monitoraggio delle operazioni), potrebbe costituire una formula idonea a garantire una vera prevenzione contro le transazioni fraudolente.

Inoltre, si avrebbero due ulteriori effetti:

- da una parte, vi sarebbe l'abbandono di una fattispecie di responsabilità oggettiva, in considerazione del fatto che con *blockchain* e IA l'intermediario ben potrebbe evitare transazioni fraudolente, senza che possa limitarsi ad allegare la mera regolarità formale delle stesse. Infatti, tecniche quali il *phishing* e similari sarebbero efficaci solo in caso di mancata adozione di queste tecnologie, con la conseguenza che sarebbe possibile ricercare profili di responsabilità soggettiva nella condotta dell'intermediario stesso il quale non abbia adottato o compiutamente/correttamente implementato tali sistemi di sicurezza;
- dall'altra parte, un impianto che prevenga le frodi anziché fornire una tutela *ex post* ha dalla sua anche il non trascurabile vantaggio di costituire uno strumento di deflazione del contenzioso davanti agli Arbitri e ai Magistrati ordinari, dal momento che assai poche sarebbero le frodi che riuscirebbero ad essere condotte a termine, dovendo superare uno "sbarramento" assai più complesso di quello che ora violano con relativa facilità.

In tal modo, da un lato si avrebbe un miglior riparto di responsabilità per i vari soggetti chiamati a operare nel caso di una transazione e, dall'altro, si otterrebbe una tutela effettiva e rapida a vantaggio dell'utente.

---

monitoraggio delle transazioni on line da parte dei correntisti (già più volte richiamato da questo Collegio; cfr., per tutte, dec. n. 1477/2011); tale dovere, infatti, consente all'intermediario di verificare il regolare andamento delle operazioni e di segnalare quelle che appaiono anomale, come è avvenuto nel caso di specie, tenuto conto che – per i bonifici di cui si discute – si tratta di operazioni effettuate in un ristretto lasso temporale e nei confronti del medesimo beneficiario, ponendosi in contraddizione con la usuale operatività del conto del ricorrente. A dimostrazione della bontà dell'assunto, va presa in considerazione la condotta tenuta dal resistente nell'immediatezza della denuncia del medesimo fatto alle autorità, in seguito alla quale ha prontamente bloccato l'ultimo dei tre bonifici contestati. La condotta tenuta, dunque, deve considerarsi contraria alla diligenza professionale, di cui all'art. 1218 cod.civ. letto in combinazione con l'art. 1176, comma 2, cod.civ., come specificamente descritta anche dalla giurisprudenza, con espresso riferimento agli intermediari bancari (cfr., tra le tante, Cass. civ., sent. nn. 20543/2009; 13777/2007, 11382/2002; 3389/2003; 6756/2001).»

EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Approvate da EMA le raccomandazioni dell'ICMRA sulla regolamentazione dell'Intelligenza Artificiale in medicina.

EMA approved the ICMRA recommendations on regulation of Artificial Intelligence in medicine.

SERGIO GUIDA
Independent Researcher, Sr. Data Governance & Privacy Mgr.

Abstract

Le tecnologie di intelligenza artificiale sono sempre più applicate in tutte le fasi del ciclo di vita di un medicinale: dalla convalida del target e l'identificazione dei biomarcatori, all'annotazione e all'analisi dei dati clinici negli studi, alla farmacovigilanza e all'ottimizzazione dell'uso clinico. Ciò comporta sfide normative, tra cui la trasparenza degli algoritmi e la loro etica, nonché i rischi di guasti dell'IA e l'impatto più ampio che questi avrebbero sulla salute dei pazienti. Due casi di studio ipotetici sviluppati nel rapporto dell'ICMRA sono stati quindi utilizzati per "sottolineare" i sistemi normativi per scoprire le aree in cui potrebbe essere necessario un cambiamento. Uno dei temi centrali riguarda le caratteristiche dell'approccio 'basato sul rischio' e il suo rapporto con l'"uomo-centrico", la cui rilevanza è stata più volte sottolineata sia da Commissione, Parlamento e Consiglio d'Europa che da EDPB e EDPS.

AI technologies are increasingly applied across all stages of a medicine's lifecycle: from target validation and identification of biomarkers to annotation and analysis of clinical data in trials, pharmacovigilance and clinical use optimisation. This brings regulatory challenges, including the transparency of the algorithms and their ethics, as well as the risks of AI failures and the wider impact these would have on patients' health. Two hypothetical case studies developed in the ICMRA's report were then used to 'stress test' the regulatory systems to discover the areas where change may be needed. One of the central topics concerns the characteristics of the 'risk based' approach and its relationship with the "human-centric", the relevance of which has been repeatedly emphasized by both the Commission, Parliament and Council of Europe and by EDPB and EDPS.

Parole chiave: EMA; etica dell'IA; trasparenza degli algoritmi; approccio basato sul rischio; umano-centrico.

Keywords: EMA; AI ethics; algorithms'transparency; risk-based approach; human-centric.

Introduzione: Intelligenza artificiale (AI) in medicina e supervisione normativa.

L'intelligenza artificiale [1] e le tecnologie di apprendimento automatico

[1] Cfr. "Possiamo, in prima battuta, definire l'intelligenza artificiale (AI) come l'insieme delle tecniche software e delle infrastrutture informatiche che, combinate insieme, permettono di portare a termine compiti con prestazioni paragonabili (a volte superiori) all'esperienza dell'intelligenza umana. (..) Le applicazioni sono presenti in tutto il '*patient journey*' del paziente: dal monitoraggio della salute individuale attraverso l'uso di dispositivi indossabili e app personalizzate per la prevenzione, all'uso di dispositivi che vengono allertati su specifici eventi in relazione ad anomalie del quadro fisiologico e alle applicazioni in grado di utilizzare dei veri e propri *virtual assistant* per supportare nelle diagnosi i medici sia nel campo generale che specialistico; particolarmente promettenti sono i software in grado di supportare le analisi di laboratorio o la diagnostica per immagini, e ancora più incredibile è lo sviluppo di sistemi di chirurgia robotica in grado di supportare chirurghi e infermieri durante gli interventi partendo dall'analisi di database di casi simili correlati a database di esiti, e come non citare le potenzialità nella riabilitazione e nei follow up dei pazienti. Di seguito alcuni esempi concreti.
Uno degli ambiti principali di applicazione dell'AI è quello dei *wearable*, con applicazioni per la prevenzione delle cadute, di predizione di attacchi cardiaci e di monitoraggio a distanza, attraverso dispositivi indossabili, di vari parametri, come il glucosio o il monitoraggio postchirurgico con *tracker* di attività. In tutte queste applicazioni sono presenti set di dati che, con meccanismi di *machine learning* o *deep learning*, vengono addestrati per riconoscere le anomalie e di conseguenza intervenire con segnalazioni opportune.
Per certi aspetti sono ancora più stupefacenti le applicazioni nel campo della diagnostica per immagini dove è possibile effettuare, ad esempio, diagnosi di patologie polmonari attraverso una semplice radiografia, diagnosi di cancro alla mammella, acquisizione di immagini e successiva ricostruzione, diagnosi di COVID 19 o screening dermatologico. In queste situazioni si sfrutta la grande maturità delle tecnologie di AI legate al riconoscimento delle immagini, soprattutto attraverso il *deep learning*.
Non è da meno il settore della medicina di laboratorio dove l'introduzione di algoritmi di AI permette il riconoscimento di patogeni e di velocizzare il sequenziamento genetico, mentre la *digital pathology*, al pari dell'*imaging*, può utilmente servirsi dei progressi di riconoscimento delle immagini.
Un altro settore assai promettente riguarda il monitoraggio fisiologico: alcune interessanti applicazioni in questo campo sono il monitoraggio dell'aderenza alle terapie, ad esempio attraverso l'analisi dei movimenti oculari in neurologia, la scansione della retina per il controllo della sclerosi multipla, il controllo della retinopatia diabetica e la prevenzione di stati di alterazione fisiologica con anticipo rispetto all'insorgenza dei sintomi. (..)
Una delle applicazioni della AI che potrebbero rivestire un impatto maggiore è quella che riguarda l'assistenza virtuale a medici e pazienti: per i primi, svolgendo compiti noiosi e ripetitivi per consentire ai medici di concentrarsi su operazioni a più elevato valore aggiunto; per i secondi, consentendo di ricevere risposte adeguate da chatbot opportunamente addestrati tramite una grande moltitudine di dati che potrebbero permettere, addirittura, di comprendere alcuni sintomi a partire dalle domande ricevute e attivando, se necessario, un sistema di allerta per particolari patologie, oltre che snellendo i processi amministrativi.
Ogni giorno sperimentiamo il lancio di nuove app nei settori più disparati e anche nel settore healthcare si osserva un enorme incremento delle app personalizzate che permettono di fornire consigli di comportamento, ad esempio nelle patologie metaboliche, fino ad arrivare ad un monitoraggio personalizzato da parte di infermieri virtuali; non si tratta di semplici gadget tecnologici, ma di un vero e proprio miglioramento dell'assistenza dei pazienti critici o cronici che richiedono una adeguata assistenza. Supportando alert, aderenza alla terapia e risposte adeguate alle domande dei pazienti, oltre a predire

hanno il potenziale per trasformare l'assistenza sanitaria ricavando nuove e importanti intuizioni dalla grande quantità di dati generati ogni giorno durante l'erogazione dell'assistenza sanitaria. I produttori di farmaci e dispositivi medici utilizzano queste tecnologie per innovare i loro prodotti per assistere meglio gli operatori sanitari e migliorare l'assistenza ai pazienti.

Il Centro per i dispositivi e la salute radiologica (CDRH) della FDA (*U.S. Food and Drug Administration*) sta da tempo considerando un quadro normativo basato sul ciclo di vita del prodotto totale per queste tecnologie che consentirebbe di apportare modifiche dall'apprendimento e dall'adattamento del mondo reale, garantendo nel contempo che la sicurezza e l'efficacia del software come dispositivo medico siano mantenuti[2].

Pochi giorni fa l'Agenzia europea per i medicinali (EMA)[3] ha approvato le

---

reazioni e seguire il follow-up, si potrà anche monitorare il livello di coinvolgimento dei pazienti e la loro esperienza per migliorare i percorsi di cura basandosi sulla storia clinica.
Ultimo esempio ma non meno importante è quello relativo alla robotica, collaborativa e chirurgica. Per la prima è interessante rimarcare la possibilità di ridurre il carico di lavoro per gli addetti ospedalieri in relazione ai compiti di routine come sanitizzare superfici, dispensare farmaci, trasportare device, ristabilire le scorte del magazzino di reparto, e si calcola che la riduzione dei costi possa arrivare al 30% dell'intera forza lavoro. In ambito chirurgico risulta molto promettente la possibilità di utilizzare dataset di procedure chirurgiche passate per sviluppare nuove tecniche riducendo il rischio di errori umani.
Questi aspetti positivi, che sicuramente sono reali e in grado di avere un benefico impatto sul sistema salute, non devono far dimenticare alcune criticità che potrebbero rallentare o addirittura far fallire l'adozione di queste applicazioni. Mi riferisco soprattutto ai problemi di qualità dei dati, di protezione dei dati e di privacy, alla cybersecurity, alla enorme quantità di dati e alla interoperabilità tra vari sistemi collettori di dati. Inoltre, molte volte non c'è trasparenza sui meccanismi di funzionamento di questi algoritmi, che possono portare a gravi bias che possono impattare in maniera drammatica sulla qualità finale dei risultati", in ALESSIO REBOLA, L'intelligenza artificiale in sanità: prospettive e rischi, Policy and Procurement in Healthcare, 31 Maggio 2021 in https://www.pphc.it/intelligenza-artificiale-in-sanita/.

[2] Cfr. "Tradizionalmente, la FDA esamina i dispositivi medici attraverso un appropriato percorso pre-mercato, come l'autorizzazione pre-mercato, la classificazione De Novo o l'approvazione pre-mercato. La FDA può anche rivedere e cancellare le modifiche ai dispositivi medici, incluso il software come dispositivo medico, a seconda del significato o del rischio rappresentato per i pazienti da tale modifica. Il paradigma tradizionale della FDA per la regolamentazione dei dispositivi medici non è stato progettato per l'intelligenza artificiale adattiva e le tecnologie di apprendimento automatico. Secondo l'attuale approccio della FDA alle modifiche del software, la FDA prevede che molte di queste modifiche al software basate sull'intelligenza artificiale e sull'apprendimento automatico a un dispositivo potrebbero richiedere una revisione pre-mercato. Il 2 aprile 2019, la FDA ha pubblicato un documento di discussione 'Quadro normativo proposto per le modifiche al software basato su intelligenza artificiale/apprendimento automatico (AI/ML) come dispositivo medico (SaMD) - Documento di discussione e richiesta di feedback' che descrive la base della FDA per un potenziale approccio alla revisione pre-marketing per l'intelligenza artificiale e le modifiche del software basate sull'apprendimento automatico", come si legge in https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.

[3] "L'Agenzia europea per i medicinali (EMA) protegge e promuove la salute dei cittadini e degli animali valutando e monitorando i medicinali all'interno dell'Unione europea (UE) e dello Spazio economico europeo (SEE). I compiti principali dell'agenzia consistono nell'autorizzare e monitorare i medicinali nell'UE. Le imprese vi si rivolgono per richiedere un'autorizzazione all'immissione in commercio unica, che viene rilasciata dalla Commissione europea. Qualora concessa, essa consente l'immissione in commercio del medicinale interessato nell'intero territorio dell'UE e del SEE. Data l'ampiezza del campo di applicazione della procedura centralizzata, la maggior parte dei medicinali veramente innovativi commercializzati in Europa viene autorizzata dall'EMA.
L'agenzia assolve i suoi compiti:
- facilitando lo sviluppo e l'accesso ai medicinali
- valutando le domande di autorizzazione all'immissione in commercio
- monitorando la sicurezza dei medicinali durante il loro intero arco di vita
- fornendo informazioni agli operatori sanitari e ai pazienti.

(..) L'EMA opera in stretta collaborazione con le autorità nazionali di regolamentazione dei paesi dell'UE e con la direzione generale della Salute della Commissione europea, una collaborazione nota come rete europea di regolamentazione dei medicinali. (..) Attraverso i suoi orientamenti scientifici, il programma di

raccomandazioni dell'*International Coalition of Medicines Regulatory Authority* (ICMRA)[4] che affrontano la supervisione normativa dell'intelligenza artificiale (AI) nello sviluppo di prodotti e tecnologie medicali.

L'intelligenza artificiale include varie tecnologie, come modelli statistici, algoritmi e sistemi automodificanti, che vengono applicati in tutte le fasi del ciclo di vita di un medicinale[5], dallo sviluppo preclinico, alla registrazione e analisi dei dati degli studi clinici[6], alla farmacovigilanza[7] e all'ottimizzazione dell'uso clinico. Secondo l'EMA, questa gamma di applicazioni comporta sfide normative, tra cui la trasparenza degli algoritmi e il loro significato, nonché i rischi di fallimenti dell'IA e l'impatto più ampio che questi avrebbero sull'adozione dell'IA nello sviluppo dei farmaci e sulla salute dei pazienti.

Il rapporto, pubblicato da ICMRA il 16 agosto, identifica le questioni legate alla regolamentazione delle terapie che utilizzano l'IA e formula raccomandazioni specifiche per i regolatori e le parti interessate coinvolte nello sviluppo dei farmaci per favorire l'adozione dell'IA.

ICMRA ha istituito una rete informale per l'innovazione che cerca di adattare i quadri regolatori per facilitare l'accesso sicuro e tempestivo ai farmaci innovativi. Come parte di questo, la 'scansione dell'orizzonte' (*horizon scanning*)[8] viene utilizzata per identificare argomenti impegnativi e sviluppare

---

consulenza scientifica e gli incentivi facilita la ricerca sui nuovi medicinali e ne favorisce lo sviluppo, traducendo in tal modo i progressi della scienza medica in farmaci che giovano realmente alla salute dei pazienti", come si legge alla pagina istituzionale https://europa.eu/european-union/about-eu/agencies/ema_it.

[4] L' International Coalition of Medicines Regulatory Authority (ICMRA) è un'entità volontaria, a livello esecutivo, di coordinamento strategico, advocacy e leadership delle autorità di regolamentazione che lavorano insieme per

- affrontare le sfide normative e di sicurezza della medicina umana attuali ed emergenti a livello globale, strategicamente e in modo continuo, trasparente, autorevole e istituzionale
- fornire indicazioni per aree e attività comuni a molte missioni delle autorità di regolamentazione
- identificare aree di potenziali sinergie
- ove possibile, sfruttare iniziative/abilitatori e risorse esistenti.

ICMRA fornirà un'architettura globale per supportare una migliore comunicazione, condivisione di informazioni, risposta alle crisi e affrontare questioni di scienza normativa, come si legge al sito web: http://www.icmra.info/drupal/en.

[5] Cfr. "Prodotto medicinale: Una sostanza o una combinazione di sostanze destinata a trattare, prevenire o diagnosticare una malattia, o a ripristinare, correggere o modificare funzioni fisiologiche esercitando un'azione farmacologica, immunologica o metabolica", come si legge nel glossario EMA alla pagina web https://www.ema.europa.eu/en/glossary/medicinal-product.

[6] Secondo il glossario dell'EMA, un "Test clinico è uno studio condotto per indagare la sicurezza o l'efficacia di un medicinale. Per i medicinali per uso umano, questi studi sono condotti su volontari umani", come riportato alla pagina web https://www.ema.europa.eu/en/glossary/clinical-trial.

[7] Cfr. "Farmacovigilanza: scienza e attività relative all'individuazione, valutazione, comprensione e prevenzione degli effetti avversi o di qualsiasi altro problema correlato ai farmaci. Ulteriori informazioni sono disponibili in 'Farmacovigilanza: panoramica, https://www.ema.europa.eu/en/human-regulatory/overview/pharmacovigilance-overview'. ", https://www.ema.europa.eu/en/glossary/pharmacovigilance. La farmacovigilanza "è la scienza e le attività relative all'individuazione, valutazione, comprensione e prevenzione degli effetti avversi o di qualsiasi altro problema correlato ai farmaci. L'Agenzia europea per i medicinali (EMA) coordina il sistema di farmacovigilanza dell'Unione europea (UE) e gestisce servizi e processi a supporto della farmacovigilanza nell'UE", come riportato alla pagina web xxx "Il diritto dell'UE richiede pertanto a ciascun titolare di autorizzazione all'immissione in commercio, autorità nazionale competente ed EMA di gestire un sistema di farmacovigilanza. L'intero sistema di farmacovigilanza dell'UE opera attraverso la cooperazione tra gli Stati membri dell'UE, l'EMA e la Commissione europea. In alcuni Stati membri esistono centri regionali coordinati dall'autorità nazionale competente".

[8] Cfr. "È possibile utilizzare una serie di strumenti per pensare in modo strutturato ai rischi e alle opportunità future. Come notato da Daniel Flynn dell'Office of the Director of National Intelligence, questi strumenti 'sono per la pianificazione futura in un mondo in cui il futuro non può essere conosciuto'. Tali strumenti sono

casi di studio ipotetici per mettere alla prova i quadri normativi esistenti e sviluppare raccomandazioni per adattarli. Ad oggi, i membri di ICMRA hanno identificato tre di questi argomenti: la stampa 3D, l'editing genetico e l'intelligenza artificiale.

Questo rapporto descrive in dettaglio i risultati dell'esercizio di 'scansione dell'orizzonte' nell'intelligenza artificiale (AI), con rilevanza per i regolatori e le parti interessate nel panorama dello sviluppo dei farmaci. I membri del gruppo di lavoro *Informal Network for Innovation* in questo rapporto erano l'Agenzia italiana per i medicinali (AIFA), l'Agenzia danese per i medicinali (DKMA), l'Agenzia europea per i medicinali (EMA) come capogruppo di lavoro, la Food and Drug Administration (FDA) degli Stati Uniti come osservatore, Health Canada (HC), l'Autorità irlandese per la regolamentazione dei prodotti sanitari (HPRA), Swissmedic e l'Organizzazione mondiale della sanità (OMS).

1. AI nello sviluppo dei farmaci.

Le tecnologie di intelligenza artificiale sono sempre più applicate nello sviluppo dei farmaci[9]. Le opportunità di applicazione dell'intelligenza artificiale

comunemente usati per aiutare a modellare la politica in modo che le entità (come i governi o organizzazioni) sono più resilienti e in una posizione migliore per intraprendere azioni efficaci. Come spiegato dall'Ufficio di Gabinetto del Regno Unito: Non si tratta di fare previsioni, ma di indagare sistematicamente le prove sulle tendenze future. La scansione Horizon aiuta il governo ad analizzare se è adeguatamente preparato per potenziali opportunità e minacce. Ciò aiuta a garantire che le policy siano resilienti a diversi ambienti futuri. La scansione dell'orizzonte non riguarda quindi la previsione del futuro, ma si concentra sull'individuazione precoce di segnali deboli come indicatori di potenziale cambiamento. La terminologia relativa a strumenti, tecniche e processi rilevanti coinvolti nella scansione dell'orizzonte deve ancora essere standardizzata, il che può portare a confusione. In alcuni casi, ad esempio, il processo complessivo di riflessione strutturata sul futuro è indicato come 'scansione dell'orizzonte' (UK Government Office for Science, 2013), mentre in altri è definito 'previsione' o 'pensiero/i futuro/i' (FAO, 2013). In questo rapporto, il comitato ha adottato una definizione simile a quella utilizzata dall'Organizzazione per la cooperazione e lo sviluppo economico (OCSE): la scansione dell'orizzonte è 'una tecnica per rilevare i primi segni di sviluppi potenzialmente importanti attraverso un esame sistematico di potenziali minacce e opportunità, con enfasi sulle nuove tecnologie e sui loro effetti sul problema in questione'.
La scansione Horizon può essere integrata in un più ampio quadro di previsione o previsione del futuro. Questo quadro descrive il processo complessivamente più ampio di valutazione e comprensione delle implicazioni politiche degli sviluppi rilevanti, nonché di identificare i futuri desiderati e le azioni politiche specifiche che possono aiutare a realizzarli. L'ETH di Zurigo ha sviluppato un modello di processo di previsione come parte degli sforzi per rafforzare il processo decisionale in Svizzera (Habegger, 2009). Questo modello ha tre fasi. Il primo prevede l'identificazione e il monitoraggio di questioni, tendenze, sviluppi e cambiamenti rilevanti, realizzati utilizzando lo strumento della scansione dell'orizzonte. La seconda fase consiste nel valutare e comprendere le sfide politiche risultanti, che si avvale di diversi strumenti. La terza fase prevede la previsione dei futuri desiderati e l'identificazione di azioni politiche specifiche per realizzarli, sulla base dello sviluppo di scenari specifici", come si legge in U.S. NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE. 2020. Safeguarding the Bioeconomy. Washington, DC: The National Academies Press, disponibile online (https://www.ncbi.nlm.nih.gov/books/NBK556429/), al cap. 6, https://www.ncbi.nlm.nih.gov/books/NBK556423/.

[9] Cfr. ad es. "Le pipeline di scoperta e sviluppo di farmaci sono lunghe, complesse e dipendono da numerosi fattori. Gli approcci di apprendimento automatico (ML) forniscono una serie di strumenti che possono migliorare la scoperta e il processo decisionale per domande ben specificate con dati abbondanti e di alta qualità. Le opportunità di applicare il machine learning si verificano in tutte le fasi della scoperta di farmaci. Gli esempi includono la convalida del target, l'identificazione di biomarcatori prognostici e l'analisi dei dati patologici digitali negli studi clinici. Le applicazioni hanno spaziato nel contesto e nella metodologia, con alcuni approcci che hanno prodotto previsioni e approfondimenti accurati. Le sfide dell'applicazione del machine learning risiedono principalmente nella mancanza di interpretabilità e ripetibilità dei risultati generati nel *machine learning*, che potrebbe limitarne l'applicazione. In tutte le aree, devono ancora essere generati dati ad alta dimensionalità sistematici e completi. Con gli sforzi in corso per affrontare questi

si verificano in tutte le fasi del ciclo di vita di un medicinale: dalla convalida del target e dall'identificazione dei biomarcatori, all'annotazione e all'analisi dei dati clinici negli studi, alla farmacovigilanza e all'ottimizzazione dell'uso clinico. Questa gamma di applicazioni comporta sfide normative, tra cui la trasparenza degli algoritmi stessi e il loro significato[10], nonché i rischi di guasti dell'IA e l'impatto più ampio che questi avrebbero sulla sua diffusione nello sviluppo farmaceutico e, in definitiva, sulla salute dei pazienti.

2. Casi di studio.

Per chiarire alcune delle sfide che l'uso dell'IA pone alla regolamentazione globale dei farmaci, i membri dell'ICMRA hanno sviluppato due casi di studio ipotetici: una "App del sistema nervoso centrale" e "Gestione del segnale di farmacovigilanza" che utilizzano entrambe l'intelligenza artificiale.

Questi esempi sono stati quindi utilizzati per "sottolineare" i sistemi normativi dei membri dell'ICMRA per scoprire le aree in cui potrebbe essere necessario un cambiamento. Il rapporto descrive in dettaglio i metodi utilizzati e i risultati, come riassunto di seguito.

Caso 1: l'intelligenza artificiale nello sviluppo e nell'uso della medicina clinica - Un'app del sistema nervoso centrale.

- Indicazione: disturbo neurodegenerativo, ad es. Parkinson o Alzheimer
- Necessità mediche: le app potrebbero avere un vantaggio rispetto al monitoraggio occasionale degli operatori sanitari offrendo informazioni sui sottili cambiamenti nei pazienti prodromici, consentendo il reclutamento di pazienti presintomatici o il monitoraggio dell'effetto

problemi, oltre a una maggiore consapevolezza dei fattori necessari per convalidare gli approcci ML, l'applicazione del ML può promuovere il processo decisionale basato sui dati e ha il potenziale per accelerare il processo e ridurre i tassi di fallimento nella scoperta di farmaci e sviluppo", come si legge in VAMATHEVAN, J., CLARK, D., CZODROWSKI, P. *ET AL*. Applications of machine learning in drug discovery and development. *Nat Rev Drug Discov* 18, 463–477 (2019). https://doi.org/10.1038/s41573-019-0024-5, 463.

[10] Cfr. "L'utilizzo sempre più diffuso degli algoritmi, a vari livelli e in diversi settori, presenta il rischio di decisioni discriminatorie e irragionevoli, con delicate implicazioni anche di carattere sociale, laddove non si conoscano e non si riescano a disciplinare i meccanismi posti alla base dell'effettivo funzionamento della 'scatola nera'. Di qui l'invito rivolto dal Parlamento britannico al governo a prendere iniziative in merito. In un rapporto su 'Algorithms in decision-making' pubblicato lo scorso 23 maggio, il Comitato 'Scienza e tecnologia' della Camera dei Comuni ha opportunamente ricordato che la tecnologia deve essere utilizzata per migliorare la qualità dei servizi pubblici e guidare l'innovazione, in particolare in settori come i trasporti e la sanità. Alla base di tutti vi sono i dati, soprattutto quelli in mano al settore pubblico, sui quali operano algoritmi che non sono affatto la formula magica che produce automaticamente benefici in assenza di un quadro accurato di regole, anche di carattere etico. In sostanza, il rapporto evidenzia che l'applicazione degli algoritmi, al pari di ogni decisione umana, può essere condizionata da errori che comportano esiti imprevedibili e talora discriminatori, soprattutto nei confronti di determinate categorie sociali, se il loro funzionamento non è corretto oppure viene alterato. Per evitare tale rischio, il Parlamento invita il governo ad affidare al *Centre for Data Ethics and Innovation* (https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about), il compito di verificare il funzionamento degli algoritmi. Il che significa controllare e garantire la qualità dei dati sui quali gli stessi si basano assicurandosi che i loro sviluppatori siano in grado di spiegare come funzionano. Tali meccanismi dovrebbero infatti essere pubblicati e conoscibili a tutti, nel momento in cui incidono sui diritti e la libertà dei cittadini", come si legge in ALESSANDRO ALONGI, Intelligenza artificiale, algoritmi e trasparenza. La lezione britannica, Lab Parlamento - Quotidiano di analisi e scenari politici, 27 Giugno 2018 in https://www.labparlamento.it/intelligenza-artificiale-algoritmi-trasparenza-la-lezione-britannica/.

dei farmaci modificanti la malattia.

- Descrizione: un'app per smartphone del sistema nervoso centrale (SNC) che misura una varietà di variabili neurologiche per replicare e basarsi su strumenti diagnostici standard aurei esistenti, ad es. velocità, movimento, memoria ecc. È anche collegato alle cartelle cliniche elettroniche. Utilizzando questi dati, applica l'intelligenza artificiale e le statistiche bayesiane, per cercare associazioni tra le variabili, la progressione della malattia e il trattamento.
- Un'ipotetica azienda desidera utilizzarlo negli studi clinici per selezionare pazienti con sintomi prodromici e monitorare la loro progressione. Dopo l'approvazione, l'azienda desidera utilizzarlo nel lungo termine per monitorare costantemente l'efficacia, l'aderenza e la risposta. Sperano che ciò consentirà aggiustamenti della dose e la dimostrazione dell'efficacia (e quindi del valore). L'app provvederà ad aggiornare regolarmente, suggerendo regimi di dosaggio migliorati, metodi di test migliorati e misure più solide del rapporto rischio/beneficio.
- Uso dell'intelligenza artificiale: utilizzerà le reti neurali per creare correlazioni tra una serie di misure neurologiche, trattamenti, caratteristiche del paziente e cartelle cliniche. Questo dovrebbe servire a migliorare i suoi consigli diagnostici, prognostici e terapeutici.
- Aspetti da implementare: la convalida clinica dell'app, come parte della sua valutazione di conformità, sarebbe necessaria per i suoi usi che incidono sul rapporto rischio/beneficio di un medicinale. Questa convalida richiederebbe un certo livello di comprensibilità o spiegabilità e potrebbe richiedere l'accesso all'algoritmo e ai set di dati sottostanti da parte delle autorità di regolamentazione. Tuttavia, potrebbe non essere possibile convalidare completamente l'App con approcci convenzionali; potrebbero essere necessari approcci più sofisticati come l'analisi del comportamento delle macchine[11]. Gli aggiornamenti al

[11] Cfr. "Ci sono tre motivazioni primarie per la disciplina scientifica del comportamento della macchina.
In primo luogo, nella nostra società operano vari tipi di algoritmi e gli algoritmi hanno un ruolo sempre più importante nelle nostre attività quotidiane. In secondo luogo, a causa delle proprietà complesse di questi algoritmi e gli ambienti in cui operano, alcuni dei loro attributi e i comportamenti possono essere difficili o impossibili da formalizzare analiticamente. Terzo, a causa della loro ubiquità e complessità, prevedere gli effetti di algoritmi intelligenti sull'umanità, positivi o negativi che siano, rappresenta una sfida sostanziale. (..) L'estrema diversità di questi sistemi di intelligenza artificiale, unita alla loro ubiquità, assicurerebbe di per sé che lo studio del comportamento di tali sistemi rappresenti una sfida formidabile, anche se i singoli algoritmi stessi fossero relativamente semplici. La complessità dei singoli agenti di intelligenza artificiale è attualmente elevata e in rapido aumento. Sebbene il codice per specificare l'architettura e l'addestramento di un modello possa essere semplice, i risultati possono essere molto complessi, spesso risultando effettivamente in 'scatole nere'. Ricevono input e producono output, ma gli esatti processi funzionali che generano questi output sono difficili da interpretare anche per gli stessi scienziati che generano gli algoritmi stessi, sebbene si stiano facendo progressi nell'interpretabilità. Inoltre, quando i sistemi apprendono dai dati, i loro errori sono collegati a imperfezioni nei dati o al modo in cui i dati sono stati raccolti, il che ha portato alcuni a sostenere meccanismi di segnalazione adattati per set di dati e modelli. La dimensionalità e la dimensione dei dati aggiungono un ulteriore livello di complessità alla comprensione del comportamento della macchina. A complicare ulteriormente questa sfida è il fatto che gran parte del codice sorgente e la struttura del modello per gli algoritmi più utilizzati nella società sono proprietari, così come i dati su cui vengono addestrati questi sistemi. Il segreto industriale e la protezione legale della proprietà intellettuale spesso circondano il codice sorgente e la struttura del modello. In molti contesti, gli unici fattori pubblicamente osservabili sui sistemi di IA industriali sono i loro input e output. Anche quando disponibile, il codice sorgente o la struttura del modello di un'IA agente può fornire un potere predittivo insufficiente

software o all'hardware dell'IA richiederebbero un nuovo test o studi di collegamento per garantire la riproducibilità/convalida. Qualsiasi modifica che influisca sul beneficio/rischio del medicinale può quindi richiedere la presentazione di nuova documentazione ad es. per una variazione all'autorizzazione all'immissione in commercio. Il test da eseguire è responsabilità dello sviluppatore, il quale. idealmente, dovrebbe avere strutture di *governance* rafforzate per supervisionare e comprendere l'algoritmo in evoluzione e garantire in continuo la gestione dei dati, la sicurezza e la privacy.

In particolare:

- *Governance*

La governance del processo di sviluppo dell'IA dovrebbe basarsi su un sistema di qualità che garantisca, come per i medicinali, standard di qualità dell'apprendimento automatico lungo l'intero ciclo di vita del prodotto, dagli studi clinici alla fase di post approvazione. Ciò potrebbe includere un comitato di supervisione multidisciplinare per comprendere l'algoritmo in evoluzione.

- *Sicurezza e privacy dei dati*

L'app dovrebbe aderire al GDPR e ad altre leggi sulla protezione dei dati applicabili, come le leggi nazionali sulla protezione dei dati. Dovrebbe anche rispettare gli standard di sicurezza informatica, ad es. secondo la Guida 29 del gruppo di coordinamento dei dispositivi medici (MDCG) della Commissione europea [12] o l'International Medical Device Regulators Forum [13]. In questo caso, verrebbe adottato un approccio basato sul

---

sul suo output. Gli agenti di intelligenza artificiale possono anche dimostrare nuovi comportamenti attraverso la loro interazione con il mondo e altri agenti che sono impossibili da prevedere con precisione. Anche quando le soluzioni analitiche sono descrivibili matematicamente, possono essere così lunghe e complesse da risultare indecifrabili. Inoltre, quando l'ambiente cambia, forse a causa dell'algoritmo stesso, è molto più difficile prevedere e analizzare il comportamento" in RAHWAN, I., CEBRIAN, M., OBRADOVICH, N. *ET AL*. Machine behaviour. *Nature* 568**,** 477–486 (2019). https://doi.org/10.1038/s41586-019-1138-y, 478.

[12] Cfr. "La Classificazione Nazionale dei Dispositivi medici (CND) è la classificazione italiana che raggruppa i dispositivi medici in categorie omogenee di prodotti destinati ad effettuare un intervento diagnostico terapeutico simile e sarà utilizzata nella Unione europea, appositamente revisionata e denominata EMDN. Il Gruppo di coordinamento Medical Device Coordination Group (MDCG) della Commissione europea ha infatti deciso, nella riunione del 14 febbraio 2019, di adottare la CND come nomenclatore per la banca dati europea EUDAMED, grazie alle peculiarità di struttura, finalità, fruibilità e metodologia di aggiornamento.La CND consente di avere una chiara conoscenza di un settore costituito da prodotti così numerosi ed eterogenei raggrupparli in modo omogeneo, secondo criteri che consentano un confronto tra prodotti appartenenti allo stesso segmento di classificazione, anche dal punto di vista economico. Consente, inoltre, di monitorare in maniera più efficace sia il consumo che l'uso dei dispositivi ed una migliore valutazione degli incidenti comparativamente per singole tipologie nell'ambito della vigilanza. Per quanto attiene all'impostazione complessiva della Classificazione si rinvia al testo di 'Introduzione alla Classificazione Nazionale dei Dispositivi medici', approvato con il Decreto del 2005 insieme alla Classificazione stessa", come riportato alla pagina web https://www.salute.gov.it/portale/temi/p2_6.jsp?id=328&area=dispositivi-medici&menu=registrazione.

[13] "Creato nel febbraio 2011, l'International Medical Device Regulators Forum (IMDRF) è un forum di regolatori volontari di dispositivi medici di tutto il mondo che si sono uniti per costruire sul forte lavoro fondamentale della Global Harmonization Task Force sui dispositivi medici (GHTF), e accelerare l'armonizzazione e la convergenza normativa internazionale sui dispositivi medici", come riportato al sito http://www.imdrf.org/. Dove si legge anche "GHTF è stato concepito nel 1992 nel tentativo di raggiungere una maggiore uniformità tra i sistemi normativi nazionali sui dispositivi medici. Ciò è stato fatto con due obiettivi in mente: migliorare la sicurezza dei pazienti e aumentare l'accesso a tecnologie mediche sicure,

rischio, che richiederebbe misure di sicurezza informatica più rigorose, segnalazioni e aggiornamenti per il software a rischio più elevato. Il sistema dovrebbe garantire la tempistica e il flusso dei dati, la catena di custodia, il tracciamento di qualsiasi modifica (ad es. tramite blockchain), la capacità di rilevare eventuali anomalie nei dati e accesso a dati di sintesi e analisi. La provenienza dei dati dovrebbe garantire che le fonti di dati siano autenticate per fornire (o ricevere) dati e metadati associate.

- *Gestione dei dati di nuovi e vecchi dati*

Sarebbe necessario un piano di gestione dei dati prima dell'autorizzazione all'immissione in commercio iniziale. Alimentare ("insegnare") l'algoritmo con nuovi set di dati di addestramento (reali), provenienti dal dispositivo dell'utente o basati su set di dati di cartelle cliniche elettroniche, richiederebbe un processo e una supervisione concordati basati sul rischio. Ciò includerebbe piani per l'azienda di acquisire, preparare e utilizzare set di dati di formazione per migliorare l'intelligenza artificiale.

Caso 2: AI e Farmacovigilanza. Gestione dei segnali di farmacovigilanza.

- Descrizione: l'industria e le autorità di regolamentazione stanno pianificando di utilizzare l'intelligenza artificiale per fornire ed elaborare i dati normativi. Un settore è la farmacovigilanza, in cui alcune autorità di regolamentazione e aziende stanno sperimentando l'IA per elaborare i dati di farmacovigilanza dalla letteratura e dai segnali Altre aree includono l'utilizzo di dati reali sulle interazioni farmaco-farmaco o farmaco-malattia, l'efficacia post-approvazione, ecc. Un' ipotetica azienda farmaceutica ha chiesto di adempiere ai propri obblighi di farmacovigilanza tramite un sistema di intelligenza artificiale, esaminando sia la letteratura che i segnali. La società ha affermato che se non è consentito utilizzare questo sistema, dovrà ritirare il prodotto dal mercato a causa di considerazioni sui costi.
- Uso dell'intelligenza artificiale: i metodi di apprendimento automatico, inclusa l'elaborazione del linguaggio naturale) nell'ipotetica intelligenza artificiale sono formati da specialisti di farmacovigilanza utilizzando un ampio set di dati bibliografici e di addestramento del segnale esistente. È stato creato un dizionario dei termini di ricerca del segnale da 'nuvole di tag'[14] per 1) sostanze medicinali sperimentali, 2) indicazioni e 3) eventi avversi. Le informazioni sono ottenute dal software attraverso il

efficaci e clinicamente vantaggiose in tutto il mondo. Una partnership tra le autorità di regolamentazione e l'industria regolamentata, la GHTF era composta da cinque membri fondatori: Unione Europea, Stati Uniti, Canada, Australia e Giappone. La presidenza è stata ruotata tra i Soci Fondatori".

[14] Il *tag cloud* (letteralmente nuvola di etichette) "è un insieme di parole chiave utilizzate all'interno del sito. E' un codice di comunicazione visuale molto utilizzato nel 'web 2.0'. Ad ogni pagina (o in generale ad ogni contenuto informativo del sito) vengono assegnate delle etichette (o parole chiave) predefinite. Più sono numerose le pagine 'taggate' con una determinata parola e più grande questa risulterà nel box. È un utile supporto alla navigazione. Infatti, i tag sono dei link che se cliccati visualizzano l'elenco dei contenuti informativi etichettati con quella parola", come riportato alla pagina web https://web.archive.org/web/20111230005700/http://www.tecnoteca.com/tecnopedia/sistemi-di-navigazione.

controllo di pubblicazioni e segnali, che sono stati filtrati e classificati per rilevanza. Sono stati condotti una serie di studi di confronto tra i risultati ottenuti tramite la ricerca manuale rispetto a quella automatica.

- La macchina aveva una sensibilità del 100% e identificava regolarmente il numero di segnali rilevanti.
- Gli algoritmi di apprendimento automatico sono stati testati con diversi altri set di dati che mostrano una sensibilità e una specificità simili, oltre a ciò in cui l'azienda e la letteratura suggeriscono i risultati dello screening umano.
- Aspetti da implementare: con l'uso previsto, questo software potrebbe essere potenzialmente classificato come dispositivo medico. La formulazione in *Good Pharmacovigilance Practices* (GVP) è ampia e descrive i requisiti minimi per la farmacovigilanza, ad esempio la ricerca della letteratura globale almeno settimanale, nonché i database consigliati, ad es. Medline o Embase e considerazioni per la precisione e il richiamo. Ciò fornisce un notevole livello di flessibilità normativa; tuttavia, può anche contribuire alle difficoltà nell'assicurare la conformità e nel citare i risultati ove richiesto. Ad es., le attuali linee guida non delineano i requisiti di tale software in dettaglio, tuttavia, per I.B.8 del modulo I GVP[15], i sistemi IT utilizzati nella farmacovigilanza dovrebbero essere idonei allo scopo e soggetti a adeguate attività di verifica, qualificazione e/o validazione per comprovarne l'idoneità.

In particolare:

- *Governance*

In questo caso l'azienda richiederebbe competenze specialistiche: anche nell'intelligenza artificiale, nella qualità dei dati e nel rilevamento del segnale di farmacovigilanza. La necessità di competenze specialistiche esterne può aumentare il rischio di conflitti di interesse tra i diversi partecipanti e le società esterne. Ciò comporterebbe chiarezza sui proprietari dei dati e su come i dati possono essere condivisi (diritti d'autore, ecc.). Se l'AI è gestita da una terza parte, dovrebbero essere garantite che questa terza parte non si sottrae a nessuna delle responsabilità dello *sponsor* e che lo strumento potrebbe essere ispezionato dalle autorità di regolamentazione.

- *Sicurezza e privacy dei dati*

I dati di farmacovigilanza sono molto sensibili dal punto di vista della protezione dei dati in quanto vi sono identificativi del paziente all'interno dei dati. Il sistema avrebbe bisogno di appropriate misure di sicurezza e la condivisione delle informazioni deve anche proteggere dall'identificazione delle persone. Dovrebbe naturalmente aderire a tutta la legislazione UE e nazionale sulla protezione dei dati applicabile.

[15] Come si legge in EUROPEAN MEDICINES AGENCY AND HEADS OF MEDICINES AGENCIES, Guideline on good pharmacovigilance practices (GVP) – Module I, EMA/541760/2011 Pag. 7/25, in https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-good-pharmacovigilance-practices-module-i-pharmacovigilance-systems-their-quality-systems_en.pdf.

3. Raccomandazioni chiave.

- Prendere in considerazione un gruppo di lavoro ICMRA permanente sull'IA per condividere esperienze di regolamentazione dell'uso dell'IA da parte degli sviluppatori e le migliori pratiche per il suo utilizzo all'interno delle stesse agenzie.

- I regolatori potrebbero dover elaborare un approccio basato sul rischio per valutare e regolamentare l'IA, attraverso lo scambio e la collaborazione nell'ICMRA. La convalida scientifica o clinica dell'uso dell'IA richiederebbe un livello sufficiente di comprensibilità e accesso normativo agli algoritmi impiegati e ai set di dati sottostanti. Potrebbe essere necessario adattare i quadri legali e normativi per garantire tali opzioni di accesso. Inoltre, possono essere individuati e tollerati limiti alla convalida e alla prevedibilità quando, ad esempio, l'IA deve apprendere, adattarsi o evolversi in modo autonomo (sul dispositivo di ciascun utente, come nel caso ipotetico 1);

tali implementazioni sarebbero anche considerate usi dell'AI ad alto rischio[16]

[16] Come noto, lo scorso 21 aprile la COMMISSIONE EUROPEA ha presentato una proposta di Regolamento ("Regulation on a european approach for artificial intelligence", disponibile alla pagina web https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206) per armonizzare le norme sull'intelligenza artificiale (IA) in Europa. Si tratta del primo quadro giuridico sull'IA che ne affronta i rischi e punta a trasformare l'Europa nel polo mondiale per un'intelligenza artificiale affidabile e che si pone sulla scia del GDPR. Come si legge alle pagine 14-16, "Il titolo III contiene regole specifiche per i sistemi di IA che creano un rischio alto per la salute e la sicurezza o per i diritti fondamentali delle persone fisiche. In linea con un approccio basato sul rischio, tali sistemi di IA ad alto rischio sono consentiti sul mercato europeo subordinatamente al rispetto di determinati requisiti obbligatori e ad una valutazione della conformità ex ante. La classificazione di un sistema di IA come ad alto rischio si basa sulla sua finalità prevista, in linea con la normativa vigente dell'UE in materia di sicurezza dei prodotti. Di conseguenza la classificazione come ad alto rischio non dipende solo dalla funzione svolta dal sistema di IA, ma anche dalle finalità e modalità specifiche di utilizzo di tale sistema. Il capo 1 del titolo III fissa le regole di classificazione e individua due categorie principali di sistemi di IA ad alto rischio:

- i sistemi di IA destinati ad essere utilizzati come componenti di sicurezza di prodotti soggetti a valutazione della conformità ex ante da parte di terzi;
- altri sistemi di IA indipendenti che presentano implicazioni principalmente in relazione ai diritti fondamentali esplicitamente elencati nell'allegato III.

Tale elenco di sistemi di IA ad alto rischio di cui all'allegato III contiene un numero limitato di sistemi di IA i cui rischi si sono già concretizzati o potrebbero concretizzarsi nel prossimo futuro. Al fine di assicurare che il regolamento possa essere adattato agli usi e alle applicazioni emergenti dell'intelligenza artificiale, la Commissione può ampliare l'elenco dei sistemi di IA ad alto rischio utilizzati all'interno di alcuni settori predefiniti, applicando una serie di criteri e una metodologia di valutazione dei rischi.
Il capo 2 definisce i requisiti giuridici per i sistemi di IA ad alto rischio in relazione a dati e governance dei dati, documentazione e conservazione delle registrazioni, trasparenza e fornitura di informazioni agli utenti, sorveglianza umana, robustezza, accuratezza e sicurezza.
I requisiti minimi proposti costituiscono già lo stato dell'arte per numerosi operatori diligenti e rappresentano il risultato di due anni di lavoro preparatorio, derivato dagli orientamenti etici del gruppo di esperti ad alto livello sull'intelligenza artificiale (https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai). Tali requisiti sono altresì in gran parte coerenti con altre raccomandazioni e altri principi internazionali, circostanza questa che assicura che il quadro dell'IA proposto sia compatibile con quelli adottati dai partner commerciali internazionali dell'UE. Le soluzioni tecniche precise atte a conseguire la conformità a tali requisiti possono essere previste mediante norme o altre specifiche tecniche o altrimenti essere sviluppate in conformità alle conoscenze ingegneristiche o scientifiche generali, a discrezione del fornitore del sistema di IA. (..) Il capo 3 definisce una serie chiara di obblighi orizzontali per i fornitori di sistemi di IA ad alto rischio. Obblighi proporzionati sono imposti anche a utenti e altri partecipanti lungo la catena del valore dell'IA (ad esempio importatori, distributori, rappresentanti autorizzati).
Il capo 4 definisce il quadro per gli organismi notificati che saranno coinvolti come terze parti indipendenti nelle procedure di valutazione della conformità, mentre il capo 5 spiega in dettaglio le procedure di valutazione della conformità da seguire per ciascun tipo di sistema di IA ad alto rischio. L'approccio di valutazione della conformità mira a ridurre al minimo l'onere per gli operatori economici e per gli organismi notificati, la cui capacità deve essere aumentata progressivamente nel corso del tempo. I sistemi di IA

[17].

- Le autorità di regolamentazione dovrebbero riunire o impegnarsi con le reti dei comitati etici esistenti e i gruppi di esperti di IA, per collaborare su questioni etiche dell'IA nello sviluppo, nell'uso e nella regolamentazione dei farmaci.

- Gli sponsor, gli sviluppatori e le aziende farmaceutiche dovrebbero istituire strutture di governance rafforzate per supervisionare l'implementazione di algoritmi e AI che sono strettamente collegati al beneficio/rischio di un medicinale, come l'automazione della conduzione della sperimentazione o utilizzo del prodotto in base ai singoli algoritmi basati sui dati. Durante lo sviluppo del prodotto dovrebbe essere istituito un comitato di supervisione multidisciplinare per comprendere e gestire le implicazioni dell'IA ad alto rischio. Gli operatori sanitari dovrebbero essere coinvolti tempestivamente ed essere pienamente informati su come l'intelligenza artificiale e gli algoritmi monitorano i pazienti e influenzano il loro uso di farmaci.

- Le autorità di regolamentazione dovrebbero considerare di stabilire il concetto di persona qualificata responsabile della conformità alla supervisione dell'IA/degli algoritmi (simile alle persone fisiche legalmente responsabili per i

---

destinati a essere utilizzati come componenti di sicurezza di prodotti disciplinati conformemente al nuovo quadro normativo (ad esempio macchine, giocattoli, dispositivi medici, ecc.) saranno soggetti agli stessi meccanismi di conformità e applicazione ex ante ed ex post dei prodotti di cui sono un componente. La differenza fondamentale consiste nel fatto che i meccanismi ex ante ed ex post assicureranno la conformità non soltanto ai requisiti stabiliti dalla normativa settoriale, ma anche a quelli fissati dal presente regolamento. (..) Dopo aver effettuato la pertinente valutazione della conformità, il fornitore dovrebbe registrare tali sistemi di IA ad alto rischio indipendenti in una banca dati dell'UE che sarà gestita dalla Commissione al fine di aumentare la trasparenza nei confronti del pubblico e la sorveglianza, nonché di rafforzare il controllo ex post da parte delle autorità competenti. (..) Le nuove regole saranno applicate direttamente e nello stesso modo in tutti gli Stati membri, sulla base di una definizione di IA adeguata alle esigenze future, e seguono un approccio basato sul rischio, che si articola in diverse fasce di pericolosità:

- per 'rischio inaccettabile' si intende i sistemi di IA considerati una chiara minaccia per la sicurezza, i mezzi di sussistenza e i diritti delle persone, che saranno vietati. La Commissione UE porta come esempi i giocattoli che utilizzano l'assistenza vocale per incoraggiare i comportamenti pericolosi dei minori e i sistemi che consentono ai governi di attribuire un 'punteggio sociale'.
- Sono considerati a 'rischio alto' i sistemi in cui la tecnologia di IA è utilizzata in infrastrutture critiche, nell'istruzione o formazione professionale, in componenti di sicurezza dei prodotti, in servizi pubblici e privati essenziali, nella gestione della migrazione, dell'asilo e del controllo delle frontiere e nell'amministrazione della giustizia e nei processi democratici.
- Sono a 'rischio limitato' i sistemi di IA con specifici obblighi di trasparenza (come i chatbot) e a 'rischio minimo' applicazioni quali videogiochi o filtri spam basati sull'IA (la grande maggioranza dei sistemi di IA rientra in quest'ultima categoria). I sistemi di IA ad alto rischio saranno soggetti a obblighi rigorosi, come adeguati sistemi di valutazione e attenuazione dei rischi, registrazione delle attività per garantire la tracciabilità dei risultati, appropriate misure di sorveglianza umana. Le aziende che non si conformeranno alle norme UE potrebbero incorrere in sanzioni fino al 6% del loro fatturato.

[17] Cfr. anche "La Commissione associa il rischio elevato a sistemi e tecnologie di IA utilizzati nell'ambito: delle infrastrutture critiche che, attraverso un algoritmo IA, potrebbero mettere a rischio la vita e la salute dei cittadini; della formazione scolastica o professionale, determinando l'accesso all'istruzione o al percorso professionale sulla base di punteggi definiti da un algoritmo IA; dei componenti di sicurezza dei prodotti (ad esempio, nella chirurgia robotica); dell'occupazione, gestione dei lavoratori e accesso al lavoro autonomo per mezzo di software IA che categorizzano CV per procedure di assunzione; dei servizi privati e pubblici in cui un algoritmo IA nega l'opportunità di ottenere un prestito; delle Forze dell'Ordine, con algoritmi che interferiscono con i diritti fondamentali dell'essere umano, ad esempio, attraverso valutazioni circa l'affidabilità delle prove di reato; della gestione della migrazione, dell'asilo politico e dei controlli alle frontiere per mezzo di sistemi IA che verificano l'autenticità dei documenti di viaggio; dell'amministrazione della giustizia e dei processi mediante algoritmi IA che applicano la legge a una serie concreta di fatti" in Giovanni De Gregorio, Federica Paolucci, Oreste Pollicino, L'intelligenza artificiale made in Ue è davvero "umano-centrica"? I conflitti della proposta, Agenda Digitale, 22 Lug 2021 in https://www.agendadigitale.eu/cultura-digitale/lintelligenza-artificiale-made-in-ue-e-davvero-umano-centrica-i-conflitti-della-proposta/.

dispositivi medici o la farmacovigilanza).

- Le linee guida normative per lo sviluppo e l'uso dell'IA con i medicinali dovrebbero essere sviluppate in una serie di aree, tra cui provenienza dei dati, affidabilità, trasparenza e comprensibilità, validità sviluppo e uso a fini di farmacovigilanza, prestazioni mondiali e monitoraggio.
- I regolatori dovrebbero sostenere lo sviluppo internazionale e la standardizzazione di buone pratiche di apprendimento automatico nel dominio biomedico.
- Nell'UE, per affrontare la natura rapida, imprevedibile e potenzialmente opaca degli aggiornamenti dell'IA, potrebbe essere necessario adattare la gestione post-autorizzazione dei medicinali, compreso il quadro di variazione, per accogliere gli aggiornamenti del software dell'IA collegato a un medicinale. Può essere vantaggioso definire aggiornamenti maggiori o minori, in un approccio basato sul rischio, per tutti gli strumenti digitali che incidono sulla qualità, sicurezza o efficacia di un medicinale e quindi legati ai suoi benefici e rischi.

Conclusions: Prossimi passi.

EMA e ICMRA sperano che questo rapporto sia utile per le parti interessate nel panorama dell'AI in medicina. L'attuazione delle raccomandazioni sarà discussa all'ICMRA. Le autorità di regolamentazione membri dell'ICMRA saranno responsabili del loro approccio all'attuazione.

Come visto il 21 aprile 2021 la Commissione Europea ha presentato la sua Proposta di Regolamento del Parlamento Europeo e del Consiglio recante norme armonizzate in materia di intelligenza artificiale. Il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (EDPS) hanno accolto con favore la preoccupazione del legislatore nell'affrontare l'uso dell'intelligenza artificiale (AI) all'interno dell'Unione europea e sottolineato che la proposta ha importanti implicazioni in materia di protezione dei dati[18].

EDPB ed EDPS hanno accolto con favore

- l'approccio basato sul rischio alla base della proposta. Tuttavia, questo approccio dovrebbe essere chiarito e il concetto di "rischio per i diritti fondamentali" dovrebbe essere allineato al GDPR e al Regolamento (UE) 2018/1725 (EUDPR)[19];
- la designazione del EDPS quale autorità competente e autorità di vigilanza del mercato per la supervisione delle istituzioni, agenzie e organi dell'Unione. Tuttavia, il ruolo e i compiti dovrebbero essere ulteriormente chiariti, in particolare per quanto riguarda il suo ruolo di autorità di vigilanza del mercato[20].

[18] Cfr. EUROPEAN DATA PROTECTION BOARD (EDPB) - EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021 in https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en,2.
[19] *Ibidem.*
[20] *Ibidem*, 3.

La designazione delle autorità di protezione dei dati (DPA) come autorità di controllo nazionali ai sensi dell'articolo 59 della Proposta[21] garantirebbe un approccio normativo più armonizzato e contribuirebbe all'interpretazione coerente delle disposizioni in materia di trattamento dei dati ed eviterebbe contraddizioni nella sua applicazione tra gli Stati membri. Di conseguenza, EDPB ed EDPS ritengono che "le autorità di protezione dei dati dovrebbero essere designate come autorità di controllo nazionali. Tuttavia, il ruolo e i compiti del EDPS dovrebbero essere ulteriormente chiariti, in particolare per quanto riguarda il suo ruolo di autorità di vigilanza del mercato. Inoltre, il futuro regolamento sull'IA dovrebbe stabilire chiaramente l'indipendenza delle autorità di controllo nell'assolvimento dei loro compiti di vigilanza ed esecuzione".

Per concludere, non posso non citare l'autorevolissima voce di Luciano Floridi, secondo il quale "poiché l'intelligenza artificiale diventerà sempre più importante e pervasiva, deve funzionare in modo affidabile, in modi in cui chiunque può fidarsi sarà a beneficio dell'umanità e dell'intero ambiente. L'alternativa è che l'intelligenza artificiale possa essere abusata, sovrautilizzata o sottoutilizzata. L'incertezza etica genera sia una sconsiderata assunzione di rischi che un'eccessiva cautela. Ecco perché le linee guida sono così importanti. Rappresentano un buon passo nella giusta direzione di un quadro chiaro, condiviso e socialmente preferibile per l'IA etica"[22].

Come peraltro confermato anche da un importante ricerca indipendente, mediante la quale è stata recentemente condotta in UK "un'analisi multivariata sul set di dati combinato di 12.113 individui per esplorare i fattori comportamentali che determinano la probabilità di un individuo di credere che la tecnologia digitale abbia il potenziale per essere utilizzata nella risposta all'epidemia di COVID-19. Il predittore più forte nel nostro modello è se un individuo ha fiducia che siano in atto le giuste regole e regolamenti per governare la tecnologia in modo responsabile. Questo indica una relazione forte tra fiducia nella governance e sostegno pubblico all'adozione di nuove tecnologie"[23].

---

[21] Cfr. "Articolo 59 Designazione delle autorità nazionali competenti
1. Ciascuno Stato membro istituisce o designa autorità nazionali competenti al fine di garantire l'applicazione e l'attuazione del presente regolamento. Le autorità nazionali competenti sono organizzate e gestite in modo che sia salvaguardata l'obiettività e l'imparzialità dei loro compiti e attività.
2. Ciascuno Stato membro designa un'autorità nazionale di controllo tra le autorità nazionali competenti. L'autorità nazionale di controllo agisce in qualità di autorità di notifica e di autorità di vigilanza del mercato, a meno che uno Stato membro non abbia motivi organizzativi e amministrativi per designare più di un'autorità", in COMMISSIIONE EUROPEA, Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di AI e modifica alcuni atti legislativi dell'Unione, Bruxelles, 21.4.2021, COM (2021) 206 final, cit., 79.

[22] Cfr. LUCIANO FLORIDI, Establishing the rules for building trustworthy AI. *Nat Mach Intell* 1, 261–262 (2019). https://doi.org/10.1038/s42256-019-0055-y, disponibile alla pagina web https://www.researchgate.net/publication/332974675_Establishing_the_Rules_for_Building_Trustworthy_AI, 1.

[23] Il CDEI ha pubblicato una nuova ricerca sull'uso dell'intelligenza artificiale e della tecnologia basata sui dati nella risposta al COVID-19 del Regno Unito (https://www.gov.uk/government/news/trustworthy-data-governance-will-unlock-innovation-research-suggests), evidenziando approfondimenti sugli atteggiamenti pubblici e sulle tendenze che ha identificato. Cfr. CENTRE FOR DATA ETHICS AND INNOVATION, Trustworthy data governance will unlock innovation, research suggests, 5 March 2021 in https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/967585/CDEI_COVID19_Repository_and_Public_Attitudes.pdf, 65.

HAVE COLLABORATED TO THIS ISSUE OF THE *EJPLT*

LUIGI BRUNO – Doctor of Civil Law (D.C.L.) candidate at McGill University.

ENRICO DAMIANI – Professor of Civil Law at University of Macerata.

VALERIA FALCE – Full professor of Economic Law, Jean Monnet Chair in EU Innovation Policy, DiCL Scientific Director at Università Europea di Roma.

SERGIO GUIDA – Independent Researcher, Sr. Data Governance & Privacy Mgr.

LUIGI IZZO – Ph.D. (c) in Humaities and Techonlogies: an integrated research path at Università degli Studi Suor Orsola Benincasa.

KONSTANTINOS KOUROUPIS – Assistant Professor of European and Data Rights Law at Frederick University.

ABDUL MALEK – Judicial Officer at Bangladesh Judicial Service.

JAVIER MARTÍNEZ CRUZ – Commissioner of the institute of transparency, access to public information and protection of personal data of the state of Mexico and Municipalities.

ANNA ANITA MOLLO – Research fellow at Università degli Studi di Napoli Federico II.

GIANLUCA MONTANARI VERGALLO – Associate Professor of Forensic Medicine at Università di Roma "Sapienza".

ERION MURATI – Ph.D. (c) and Lecturer at the Law Faculty of the University of Hamburg.

LUIGI FILIPPO NAPPI - Teaching Assistant in New Technology Law at Università degli Stusdi Suor Orsola Benincasa.

MARIA ROBERTA PERUGINI – IUSINTECH co-founder, Civil Lawyer expert in new technology law.

CHIARA RAUCCIO – LL.M. at Tilburg University, Lawyer.

ISABELLA SPANO – Doctor of Civil Law (D.C.L.) candidate at the Law Faculty at McGill University.

HANS STEEGE – Deputy director of the Interdisciplinary Institute of Automated Systems e.V. (RifaS), Hannover.