Essays

The 'User-Centric' and 'Tailor-Made' Approach of the GDPR Through the Principles It Lays down

Francesco Giacomo Viterbo*

Abstract

The European approach to online privacy and personal data concerns in the contemporary digital age appears to have embraced a 'user-centric' approach, inspired by values of 'personalism' and human dignity, regardless of the growing commercial value commonly given to personal data.

These two sides of the same coin have been taken into account by the GDPR. On the one hand, it seems to outline a system of protection of data subjects that presents certain similarities and connections with consumer protection directives, especially as regards the transparency principle and the aim to provide individuals with 'effective' protection, enforceable rights and awareness-raising activities. On the other hand, a radical shift in the data protection policies of big online companies and many other service providers is required by the implementation of the set of mandatory principles and obligations stated by chapter IV of the GDPR, while the notice-and-consent paradigm is now quite remote.

In particular, data minimisation, confidentiality, integrity, data protection by design and by default, as well as accountability and scalability principles require a model of approaching the new challenges brought about by data protection that should be 'contextual' and 'tailor-made'. This means that the appropriate measures to be adopted by controllers and processors must consider the specific circumstances of each individual case, in accordance with a proportionality and reasonableness test on the extent of risks to the rights and freedoms at stake.

The new legal framework provided by the GDPR and Convention 108+ has weakened the role of national laws on personal data protection but has also posed the challenge of providing a uniform legal frame, at the European Union level, as well as of strengthening the harmonisation process among countries that are currently taking different approaches to data protection at a global level.

I. Three Different Approaches to Flows of Personal Data and the New Challenges Brought About by Technological Developments

The General Data Protection Regulation (GDPR) explains its social background under Recital 6, specifying that

> '(r)apid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection

* Associate Professor of Private Law, University of Salento.

> and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally'.

The subsequent Recital 7 points out that

> '(t)hose developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market'.

Even though in recent years virtually no one has doubted that such economic and social developments, involving considerable personal data-sharing platforms in online and offline markets, require a renewed legal framework, such a viewpoint might raise a number of important questions, including: How can personal data be treated in the legal system? To whom do personal data belong? Do they belong to the data subject? Or to the controller? Or to another entity entirely? Can personal data flow in markets and online networks without any legal obligation?

During the period when the European Union (EU) data protection reform was taking shape, some authors focused on the issue concerning 'default entitlements in personal data', assuming as the starting point that

> 'how entitlements in personal data are being allocated initially, ie the default entitlements before the parties negotiate reallocation, is of special importance'.[1]

In short, an important choice had to be given by the European drafter of the reform between building a new legal framework based on the principle of informational self-determination, pursuant to which the individual take control over his/her own personal data; or, in contrast, assigning a great deal of default rights to others, including governments and/or information industries.

In a more general viewpoint, there are three fundamental approaches with regard to the legal regulation of personal data flows in the current digital age:

a) state-centric approach

b) market-centric approach

c) user-centric approach.

These are destined to have different fortunes in accordance with the cultural

[1] N. Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination Off the Table … and Back on Again?' 1 *Computer Law & Security Review*, 8 (2014). One conclusion of this analysis asserted that the proposed Regulation's draft could shift the balance away from the informational self-determination and default individual's entitlement in favour of competing (business) interests and the default entitlement of others to process personal data.

background and political, social and economic context to which we refer.

Starting from the approach *sub* a), a state-centric regulation takes place when the government uses advanced analytics to collect and process personal data on a mass scale in order to profile all citizens and shape public policy. In this viewpoint, personal data are treated like goods, having a public utility insofar as they belong to the government, which is able to process them for purposes of social utility (eg citizens' safety) or social control (including crime prevention).[2] Nonetheless, it is evident that this kind of approach poses a number of threats to equality, freedom and democracy.

The approach *sub* b) can be termed 'market-centric'. The gist of this approach is either to entitle by default data-hungry private entities or to allow the trade and sale of personal data, *de jure* or *de facto*, in order to boost the free movement of information in the market. In accordance with a market-oriented approach, personal data would have a commercial value:

> 'in a flourishing online ecology, where individuals, communities, institutions, and corporations generate content, experiences, interactions, and services, the supreme currency is information, including information about people'.[3]

The basic assumption underlying this approach to personal data is provided

[2] In accordance with a global trend, 'in recent decades, governments around the world have obligated a wide variety of businesses to collect, retain, and share data about their customers and clients to assist in curtailing money laundering, drug trafficking, tax evasion, terrorism, and other offences. Governments have sought access to personal information held by the private sector not only by asking companies to produce specific records about a single target or a small number of people at a time but increasingly via what we refer to here as "systematic" government access. As used throughout this issue, this term refers both to (1) direct access by the government to private-sector databases, without the mediation or interaction of an employee or agent of the entity holding the data, and (2) government access, whether or not mediated by a company, to large volumes of private-sector data': see F.H. Cate, J.X. Dempsey and I.S. Rubinstein, 'Systematic Government Access to Private-Sector Data' 4 *International Data Privacy Law*, 195 (2012). In this regard, we can consider the case of China's Social Credit System, a national reputation system being developed by the Chinese government in order to rate the trustworthiness of its one point three billion citizens. This system uses big data analysis technology and may be considered a form of mass surveillance. By February 2018, one such program has been implemented in Shanghai through its 'Honest Shanghai' app, which uses facial recognition software to browse government records, and rates users accordingly. In January 2019, Beijing government officially announced that it will start to test 'Personal Credit Score'. For more details, see F. Liang, V. Das, N. Kostyuk, and M. Hussain, 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure' 10 (4) *Policy & Internet*, 415-453 (2018); G. Kostka, 'China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval' 21(7) *New Media & Society*, 1565-1593 (2019). Moreover, the legality of this Social Credit System is not compromised by the new 'National Standards on Information Security Technology - Personal Information Security Specification GB/T 35273-2017' ('PI Specification') that came into force on 1 May 2018. The 'PI Specification' is not a mandatory regulation and it does not apply to Chinese public authorities, giving rise to compliance issues only for business operations in China: see B. Li, 'China Issues Personal Information Security Specification' available at https://tinyurl.com/r77ee2f (last visited 30 December 2019).

[3] H. Nissenbaum, 'A Contextual Approach to Privacy Online' 140(4) *Daedalus*, 33 (2011).

by an empirical observation of present-day practices in the marketplace and social life, especially in the online world, where large amounts of personal data change hands or even 'ownership' as part of merger-acquisitions and other strategic transactions. On the Internet, individuals usually make deals for the disclosure, collection, use and reuse of their personal data; in certain situations they receive some form of compensation and thus 'exploit' and 'sell' their habits, customer/user-profile and even sensitive personal data.[4] Indeed, personal data would be labelled 'personal' by virtue of the fact that they 'belong' to the data subject, as well as on the basis of being a property right. The precondition for applying the logic of 'propertisation' to personal data is that data can be subjected to a process of commodification that ends up equating them with any other kind of tradable commodity. The commodification of information would be inevitable, especially for consumers with regard to their personal data.[5] In addition, it is stressed that such a process would lead to a higher level of protection by taking (industrial and intellectual) property rights as a reference.[6] This means that if personal data are deemed similar to a commodity or goods that may be destined for appropriation or commercial exploitation, then the protection and circulation regime appropriate to such goods would be applicable, being loanable from copyright law and contract law.[7]

[4] G. Spindler, 'Datenschutz- und Persönlichkeitsrechte im Internet – der Rahmen für Forschungsaufgaben und Reformbedarf' *Gewerblicher Rechtsschutz und Urheberrecht*, 996 (2013).

[5] A. Bartow, 'Our Data, Ourselves: Privacy, Propertization, and Gender' 34 *University of San Francisco Law Review*, 634 (2000).

[6] Illustrative is the story of Amazon.com, analyzed by L. Lessig, 'Privacy as Property' 69 *Social Research*, 249 (2002). By selling books, Amazon was a collector of data and could build accurate profiles about its customers by monitoring their behavior. The data it was collecting, Amazon said in its privacy policy, would not be sold to others. Information was therefore collected by Amazon only to better serve its customers. At the end of 2000, however, Amazon announced a new policy. From that point on, data collected could be sold to or shared with people outside Amazon, regardless of a consumer's request that it not. Amazon also made that policy retroactive and refused requests to delete earlier data. The consumers who had relied on its policy were told they had no right to remove the data they had given: 'their data was subject to sale'. See what L. Lessig says about this story: 'If it were taken for granted that privacy was a form of property, then Amazon simply could not get away with announcing that this personal information was now theirs'; 'just imagine if we thought about our personal data the way we think about a car. And then think about this analogous case about a contract governing a car. You drive into a parking lot, and the attendant hands you a ticket. The ticket lists a number of rules and promises on the back of the ticket. The lot is not responsible for damage to the car; the car must be picked up by midnight, etc. And then imagine, as with Amazon, that at the bottom of the ticket, the last condition is that this license can be modified at anytime by the management'; 'Obviously, in ordinary property thought, this is an absurd idea. It would be crazy to interpret a condition in a license stating that the license could be changed to mean that the license might be changed to allow the parking lot to sell your car'.

[7] This approach has particularly been proposed by scholars in the United States: R.A. Posner, 'The Right of Privacy' 12 *Georgia Law Review*, 393-422 (1977); J. Litman, 'Information Privacy/Information Property' 52 *Stanford Law Review*, 1283 (2000); A. Bartow, n 5 above, 633; J. Zittrain, 'What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication' 52 *Stanford Law Review*, 1201-1250 (2000); L. Lessig, n 6 above,

In contrast, the European approach to online privacy and personal data concerns appears to differ from the above default settings. If both Directive 1995/46/EC and the recent GDPR are taken into account, the EU legal system seems to have embraced a user-centric approach inspired by values of 'personalism' and human dignity.[8]

Although some believe that it is possible to sell personal data, such an opinion leads to a false perspective. Personal data are not simply pieces of information. They refer to a particular, identified or identifiable natural person and can be capable of revealing some of the most intimate and delicate aspects of that individual's personality, such as his/her state of health or sex life. Their significance is not linked to the economic and quantitative criterion of marketability, but rather to a rationale based on the protection of human rights and freedoms.[9] This argument may be inferred from the EU personal data protection laws, wherein there is no provision for a specific contract that would allow the data subject or the data controller to dispose of personal data. A further argument is given by Recital 24 of the Directive 2019/770 'on certain aspects concerning contracts for the supply of digital content and digital services', where it is fully recognised that 'the protection of personal data is a fundamental right and that therefore *personal data cannot be considered as a commodity*'.[10] Accordingly,

247–269; P.M. Schwartz, 'Property, Privacy and Personal Data' 117 *Harvard Law Review*, 2056–2128 (2004); in Italy, see L.C. Ubertazzi, 'Banche dati e privacy' *Diritto industriale*, 633 (2002), who remarks that the right of individuals in allowing the processing of their personal data has the same legal framework of the intellectual property rights; and V. Zeno Zencovich, 'Profili negoziali degli attributi della personalità' *Diritto dell'informazione e dell'informatica*, 547 (1993). In the European debate, see Y. Poullet, 'Data Protection Between Property and Liberties. A Civil Law Approach' in H.W.K. Kaspersen and A. Oskamp eds, *Amongst Friends in Computers and Law. A Collection of Essays in Remembrance of Guy Vandenberghe* (The Hague: Kluwer Law International, 1990), 160; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002), 120; N. Purtova, *Property Rights in Personal Data: a European Perspective* (The Hague: Kluwer Law International, 2011), 1.

[8] See Recital 4 of the GDPR, which specifies that '*The processing of personal data should be designed to serve mankind*. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality' (italics added). Approaching these issues in the light of fundamental principles provided by EU Treaties and EU Member States' Constitutions is of paramount importance: see P. Perlingieri, '*Privacy* digitale e protezione dei dati personali tra persona e mercato' *Il Foro napoletano*, 481-490 (2018); Id, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti* (Napoli: Edizioni Scientifiche Italiane, 2006), 719-720; Id, *Il diritto dei contratti fra persona e mercato. Problemi del diritto civile* (Napoli: Edizioni Scientifiche Italiane, 2003), 367-370; A. Gambino, 'Dignità umana e mercato digitale' in G. Contaldi ed, *Il mercato unico digitale* (Roma: Nuova Editrice Universitaria, 2017), 7-18.

[9] F.G. Viterbo, *Protezione dei dati personali e autonomia negoziale* (Napoli: Edizioni Scientifiche Italiane, 2008), 149-152.

[10] The text of the 'Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services' is available at https://tinyurl.com/tourdtu (last visited 30 December 2019). Recital 24 specifies that this Directive applies 'to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or

there is no room for the commodification of personal data in both the wording and rationale of Arts 7 and 8 of the EU 'Charter of Fundamental Rights'.

It is precisely in this respect that personal data seem to differ from all other goods in the Italian and EU legal orders. On the one hand, they pose as elements creating the data subject's personal identity. On the other hand, personal data can serve as an important resource that may be the object, not of appropriation but rather of *access*; not for enjoyment or consumption, but rather for *processing* by third parties for specific and worthy purposes.[11]

In accordance with this user-centric approach, personal data may be deemed intangible goods, which are *not* (directly) *transferable*, within the meaning given to this term by the most important civil codes enacted in the EU context. An alternative is to regard personal data as intermediate rather than final goods, instrumental rather than ultimate values. Indeed, people are assumed not to desire or value personal data in themselves, but to use personal data by processing them in order to obtain opportunities for gain or some other measure of utility or welfare.[12] Under this approach, the only *commodifiable* and *marketable*

undertakes to provide, personal data', ensuring 'that consumers are, in the context of such business models, entitled to contractual remedies'. It is important to note that Art 3(1) of the Commission draft of this Directive (COM(2015)0634 – C8-0394/2015 – 2015/0287(COD)) referred to 'any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or *the consumer actively provides counter-performance other than money in the form of personal data or any other data*' (italics added). This draft was later modified and the final text deletes all references to the provision of personal data as a counter-performance: see European Data Protection Supervisor (EDPS), 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content', adopted on 14 March 2017 (available at https://tinyurl.com/tdjryq3 (last visited 30 December 2019)), where 'the EDPS considers that the term "data as a counter-performance" should be avoided'. For further remarks, see D. Clifford, I. Graef and P. Valcke, 'Pre-formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' 20 *German Law Journal*, 679-721 (2019); G. Finocchiaro, 'Il quadro di insieme sul Regolamento europeo sulla protezione dei dati personali' in G. Finocchiaro ed, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Bologna: Zanichelli, 2017), 2.

[11] F.G. Viterbo, n 9 above, 153-155. See also S. Spiekermann et al, 'Personal Data Markets' 25 *Electronic Markets*, 91 (2015), as they observe that personal data 'is not just an ordinary tradable asset' and 'can be highly sensitive and revealing about a person's identity'; 'processing it is legally restricted by data protection and privacy laws. In many countries, privacy and the right to information self-determination are recognized as a human right.' This viewpoint has been confirmed by G. Buttarelli in EDPS, 'Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data', 23 September 2016, para 4, where he argues that '(i)n the EU, personal information cannot be conceived as a mere economic asset'.

[12] The above analysis can be linked with the following statements stressed by R.A. Posner: 'People invariably possess information, including facts about themselves and contents of communications, that they will incur costs to conceal. Sometimes such information is of value to others: that is, others will incur costs to discover it. Thus we have two economic goods, "privacy" and "prying". We could regard them purely as consumption goods, the way economic analysis normally regards turnips or beer; and we would then speak of a "taste" for privacy or for prying. But this would bring the economic analysis to a grinding halt because tastes are unanalyzable from an economic standpoint. *An alternative is to regard privacy and prying as intermediate rather*

goods seem to be the benefits and pecuniary advantages that the data controller receives *through* and *after* the processing of personal data, provided that such processing is carried out in full compliance with personal data protection law. From this perspective, when referring to personal data, the concept of processing implies that a special set of rules has to be applied to all concerns regarding personal data and their movement in the market. This regime is wholly autonomous and does not overlap with the rules of the *ius commune* concerning the transfer of ownership and intellectual property.[13] Therefore, there is no room for entitlement in personal data as ownership, on the grounds set out above. The problem is establishing *whether* and *how* personal data may be processed in each specific concrete online or offline context.[14] That is to say, *whether* and *how* the data subject's fundamental rights may be preserved.

This user-centric approach should also be applied in the context of big data[15] and artificial intelligence (AI)-based applications.[16]

than final goods, instrumental rather than ultimate values. Under this approach, people are assumed not to desire or value privacy or prying in themselves but to use these goods as inputs into the production of income or some other broad measure of utility or welfare' (R.A. Posner, n 7 above, 394 (italics added)).

[13] F.G. Viterbo, n 9 above, 156-158. See also F. Ferretti, 'A European Perspective on Data Processing. Consent through the Re-conceptualization of European Data Protection's Looking Glass after the Lisbon Treaty: Taking Rights Seriously' *European Review of Private Law*, 481 (2012).

[14] In this regard, see the 'contextual approach' proposed by H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010), 129-244; Id, n 3 above, 33: 'I give an account of privacy in terms of expected flows of personal information, modeled with the construct of *context-relative informational norms*. The key parameters of informational norms are actors (subject, sender, recipient), attributes (types of information), and transmission principles (constraints under which information flows)'.

[15] 'Big Data represent a new paradigm in the way in which information is collected, combined and analysed. (…) In terms of data protection, the main issues concern the analysis of the data using software to extract new and predictive knowledge for decision-making purposes regarding individuals and groups': see 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data', drafted by the Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, T-PD(2017)01, adopted on 23 January 2017, paras I and III, available at https://tinyurl.com/wtzex5k (last visited 30 December 2019). In Italy, the Supervisory Authority for the protection of personal data ('*Garante* privacy'), the Competition Authority ('AGCM') and the Authority for Communications Guarantees ('AGCOM') have published the 'Big Data Guidelines and policy recommendations', on July 2019, available at https://tinyurl.com/vkefu8w (last visited 30 December 2019). On this topic see A. Mantelero, 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection' 32(2) *Computer Law & Security Review*, 238-255 (2016); C. Kuner, F.H. Cate, C. Millard and D.J.B. Svantesson, 'The challenge of 'big data' for data protection' 2(2) *International Data Privacy Law,* 47-49 (2012); N. Purtova, 'Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons', in R. Leenes, N. Purtova, S. Adams eds, *Under Observation - The Interplay Between eHealth and Surveillance* (Springer, 2017), 177; A. Soro, 'Big Data e Privacy. La nuova geografia dei poteri', *Convegno per la Giornata Europea della protezione dei dati personali 30 gennaio 2017*, available at https://tinyurl.com/qqpwlqq (last visited 30 December 2019).

[16] H. Nissenbaum, n 3 above, 33.

The reference point is given by the 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data', drafted by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108, hereafter 'Convention 108'). The purpose of these guidelines is to

> 'recommend measures that Parties, controllers and processors should take to prevent the potential negative impact of the use of Big Data on human dignity, human rights, and fundamental individual and collective freedoms'

and

> 'to contribute to the protection of data subjects regarding the processing of personal data in the Big Data context by spelling out the applicable data protection principles and corresponding practices, with a view to limiting the risks for data subjects' rights'.[17]

Moreover, one must not overlook the 'Guidelines on Artificial Intelligence and Data Protection', recently drafted by the Consultative Committee of the Convention 108, providing

> 'a set of baseline measures that governments, AI developers, manufacturers, and service providers should follow to ensure that AI applications do not undermine the human dignity and the human rights and fundamental freedoms of every individual',

in particular when AI applications are used in decision-making processes.[18]

This viewpoint seems to require not only a user-centric approach, but also a collectivity-centric approach, affording a 'meta-individual' dimension to personal data protection.

II. Harmonisation Led by the GDPR and Convention 108+: The Points of Divergence from the Past

Almost one year after the GDPR entered into force, the Council of Europe adopted the updated text of Convention 108 in order to promote at the global level the fundamental values of respect for privacy and protection of personal data, given the diversification, intensification and globalisation of data processing and personal data flows, especially in the online world. This 'modernised

[17] See para II of the above mentioned guidelines.

[18] See para I of the 'Guidelines on Artificial Intelligence and Data Protection', drafted by the Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, T-PD(2019)01, adopted on 25 January 2019, available at https://tinyurl.com/qp6r4ux (last visited 30 December 2019).

Convention' (hereinafter: Convention 108+) can be signed and ratified by any country around the world and could represent the global standard for personal data protection.

Both the GDPR and Convention 108+ are having a new impact on the harmonisation of personal data protection. The former is providing a uniform legal frame at the EU level; the latter will strengthen harmonisation among countries that currently have different levels of data protection.

Both the GDPR and Convention 108+ confirm some well-known principles applying to personal data protection, but also introduce some points of breaking with the past, such as the following:

1. The purpose of maximum harmonisation pursued through the adoption of the EU Regulation 2016/679 repealing Directive 95/46 and the introduction of cooperation mechanisms at the European and global levels;
2. A more detailed regulation of consent as a legitimate basis of the processing of personal data, except in cases 'where there is a clear imbalance between the data subject and the controller';
3. Some principles and guarantees set out by data protection law are very similar to those solutions that have already been embraced in the area of consumer law, given the increasing commercial value of personal data;
4. The *accountability* and *scalability* principles, introducing a 'contextual' and 'tailor-made' approach to personal data protection concerns, to be assessed on a case-by-case basis;
5. The pivotal role of cooperation among data scientists, scholars, lawyers and data protection supervisory authorities for the effective protection of the fundamental rights and freedoms of individuals, as well as for the global harmonisation trend.

III. The GDPR's Uniform Legal Frame Weakening the Role of National Privacy Codes: The Italian Case

In accordance with Art 288 TFEU, regulations are binding in their entirety and 'directly applicable'. Therefore, in all EU Member States, internal laws concerning personal data protection have been profoundly reformed since the GDPR uniform legal frame entered into force.[19] In Italy, illustrative is the

[19] On the GDPR as a uniform legal frame on personal data protection in the Union, see G. Finocchiaro, n 10 above, 8-9. The reason that guided the European legislator towards a new regulation in place of a new directive is probably pointed out by Recital 9 of the GDPR: Directive 95/46/EC 'has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore

reform set out by the decreto legislativo 10 August 2018 no 101, which revised and reshaped the decreto legislativo no 196/2003 (widely known as the 'privacy code', hereinafter: Code).

The above reform abolished all articles and provisions of the Code that were overlapping or inconsistent with regard to the GDPR's contents. For instance, in the new version of Art 154(1) of the Code pertaining to tasks assigned to the Italian supervisory authority (hereinafter: Garante) has been the removal of the previous clause under letter *c)* according to which one of the assigned tasks

> 'shall consist in ordering data controllers or processors, also ex officio, to adopt such measures as are necessary or appropriate for the processing to comply with the provisions in force'.

This is currently provided for by the GDPR itself, pursuant to Art 58(2)(d).

Therefore, only complementary and implementing rules have been left and/or modified in the current text of the Code.[20]

According to this perspective, for instance, Art 2-*quinquies* has implemented Arts 8(1) and 12(1) of the GDPR, admitting the processing of personal data in relation to information society services on the basis of a child's consent where the child is at least fourteen years old. Where the child is younger, the legal basis of such processing requires that consent is given or authorised by the holder of parental responsibility over the child. Moreover, in accordance with the above Articles, the controller must provide the child with all information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that is to say, user-friendly information for a younger person.

In addition, some Articles of the Code entrust the implementation of the GDPR to the *Garante*.

In this regard, it is appropriate to consider Art 2-*septies* regulating the processing of genetic data, biometric data or data concerning health in accordance with Art 9(4) of the GDPR. Such data processing must be undertaken in compliance with the specific measures laid down by the Garante.[21] One must not overlook the fact that consent given by the data subject is no longer required in order to make data processing for health purposes lawful, pursuant to Art 9(2)(h) of the GDPR.[22] This is an important novelty implemented by the Code and

constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC'.

[20] For further details see F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679* (Torino: Giappichelli, 2016), II, 13-49

[21] As regards the processing of personal data for health purposes, see Garante per la Protezione dei Dati Personali, 7 March 2019 no 55, available at www.garanteprivacy.it.

[22] Art 9(2)(h) of the GDPR refers, in particular, to data processing which 'is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of

Garante assessments.[23] Nevertheless, in the case of data processing through online medical reports, the consent given by the patient (data subject) is required by the Italian legislation as a legal basis in order to render the processing lawful.[24]

Given that definitions, principles pertaining to the processing of personal data, the rights of the data subject, obligations binding controller and processor, transfers of personal data to third countries and even administrative fines are actually contained in the GDPR and directly applicable, the material scope of the internal 'privacy code' has been weakened and its role within data protection legal sources is now quite distant.

IV. Rules and Principles Concerning the Fairness and Lawfulness of any Processing of Personal Data, Focusing on the Issue of Online Services Offered for the 'Provision of Personal Data'

Even though the fairness and lawfulness of any processing of personal data must be assessed on a case-by-case basis, such an assessment always requires an answer to the following preliminary questions: a) Is there a legitimate basis justifying the processing of personal data? b) What purpose does the processing of personal data pursue? Is the processing compatible with the purposes for which the personal data were initially collected?

It is no coincidence that in the gist of information to be provided where personal data are collected from the data subject pursuant to Art 13(1) of the GDPR, 'the *purposes of the processing* for which the personal data are intended as well as the *legal basis for the processing*' are supposed to be mentioned together.[25]

The first condition of lawfulness, ie the disclosure of a legitimate basis, means that the processing of personal data should not be unlimited insofar as it must be carried out with the *consent* of the data subject *for one or more specific purposes*, or be *necessary* in accordance with one of the other cases specified by Art 6(1) of the GDPR.[26]

Consent to process personal data can be qualified as an act of autonomy by which an individual admits others into his/her own private sphere. It is generally

the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional'.

[23] See Garante, n 21 above, para 1.

[24] See Art 5 of the DPCM 8 August 2013.

[25] See Art 13(1)(c). Italics added.

[26] Pursuant to Art 6(1) of the GDPR, such legitimate basis of data processing may occur, in particular, when the processing 'is necessary for the performance of a contract to which the data subject is party'; or when it 'is necessary for compliance with a legal obligation to which the controller is subject'; or when it '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'; or when it 'is necessary in order to protect the vital interests of the data subject or of another natural person'.

said that consent to data processing that does not expressly permit communication or dissemination of the same data has the effect of rendering lawful only those operations carried out by the data controller, without the data being able to circulate further. However, this approach is no longer appropriate to negotiating the issues and challenges we encounter in the online world today. There is considerable agreement that the paradigm of notice-and-consent has failed insofar as

> 'existing regimes have not done enough to curb undesirable practices, such as the monitoring and tracking associated with behavioral advertising and predatory harvesting of information posted on social networking sites'.[27]

For many critics, 'the fault lies with the ubiquitous regime of offering privacy to individuals on a "take it or leave it" basis'.[28] In order to tackle these concerns, the GDPR and the 'Proposal for a Regulation on Privacy and Electronic Communications' (ePrivacy Regulation) provide further safeguards, ensuring or attempting to ensure that consent could form the legitimate basis of data processing only when it is consciously and freely given by the data subject.[29]

Pursuant to Art 7(4) and Recital 43 of the GDPR, consent is not

> 'a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller'

and, in particular,

> 'consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or *if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*'.[30]

[27] H. Nissenbaum, n 3 above, 34. The need of rethinking the 'notice and consent' paradigm has been focused by many authors. In particular, see A. Mantelero, 'The future of consumer data protection in the EU. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics' 30 *Computer Law & Security Review*, 643-660 (2014); S. Thobani, 'Il consenso al trattamento dei dati personali come condizione per la fruizione di servizi online' in C. Perlingieri and L. Ruggeri eds, *Internet e Diritto civile. Atti del Convegno* (*Camerino 26 – 27 September 2014)* (Napoli: Edizioni scientifiche italiane, 2015), 459-484; A. Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale* (Napoli: Edizioni Scientifiche Italiane, 2019), 81-170.

[28] H. Nissenbaum, n 3 above, 35.

[29] For further details on the requisites for a valid consent, see the 'Guidelines on Consent under Regulation 2016/679', adopted on 28 November 2017, by the Art 29 Data Protection Working Party. On the proposal for a 'ePrivacy Regulation', which is to repeal and replace the Directive 2002/58/EC (ePrivacy Directive), see EDPS, 'Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)', adopted on 24 April 2017, available at https://tinyurl.com/vgh3pus (last visited 30 December 2019).

[30] Italics added.

This specification seems to be important especially for data protection in the online environment, where a great number of services are offered for free to end-users. 'Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader', ie by giving access to personal data or other data.[31] It follows that the request to collect and process personal data, such as for the purpose of displaying customised advertisements based on behavioural advertising technology to users, would be encompassed within the core business of the contract and accepted by the user as a form of compensation for the provision of the service offered for free.[32] In most cases, consent to the processing of personal data cannot be freely given by users. Therefore, two scenarios can be envisaged, insofar as the processing should find another legitimate basis, or otherwise be rendered unlawful.

In the first scenario, given that the provision of a commodity or service would be bound to the consent (not freely) given by a consumer to the processing of personal data for marketing purposes, the controller (for example, the editor of a website) who does not permit consumers to enjoy a service would be behaving unfairly.[33] Therefore, in such cases, the processing of personal data would never have a legitimate basis, regardless of contractual clauses admitting it. These would be unfair too.

In contrast, the second scenario is where such processing falls within the scope of either Art 6(1)(b) or Art 6(1)(f) of the GDPR.

[31] This specific 'business model' is explicitly taken into consideration by Recital 24 of the Directive (EU) 2019/770, n 10 above. On 24 March 2016, the Organisation for Economic Cooperation and Development (OECD) Council revised its 1999 Recommendation on Consumer Protection in E-commerce, including 'non-monetary transactions' in the key new developments, emerging trends and challenges faced by consumers in today's dynamic e-commerce marketplace: 'Consumers increasingly acquire "free" goods and services in exchange for their personal data and these transactions are now explicitly included in the scope of the Recommendation. Governments and stakeholders are called upon to consider ways to provide redress to consumers experiencing a problem with such transactions'. Whether and how to protect the weaker contractual party in such non-monetary online transactions is a relevant issue: for more details, see F.G. Viterbo, 'Freedom of contract and commercial value of personal data' *Contratto e impresa/Europa*, 612-619 (2016); with regard to the user's act of joining a social network, see C. Perlingieri, *Social Networks and Private Law* (Napoli: Edizioni Scientifiche Italiane, 2017), 63-98.

[32] For more details on 'the agreement concluded between the social network and the user to be conceptualised as a reciprocal contract in a legal sense concerning licences to use intangible material such as IP content and the social site's software platform', see C. Perlingieri, n 31 above, 85-91.

[33] See the '*vademecum*' called 'Up with Tips. Down with Spam. Privacy-Proof Marketing from Your Telephone to the Supermarket', which explains that the provision of a commodity or service cannot be bound to the consumer's consent to the processing of personal data for the purpose of sending ads: Garante per la Protezione dei Dati Personali 20 April 2015, available at www.garanteprivacy.it. Moreover, in presence of dominance in competition law terms, the controller could abuse its dominant position in the market by infringing data protection rules: on this point see N. Zingales, 'Between a Rock and Two Hard Places: WhatsApp at the Crossroad of Competition, Data Protection and Consumer Law' 33 *Computer Law & Security Review*, 555-556 (2017).

The former solution is the case where the legal ground for making data processing legitimate is the conclusion and performance of a contract.[34] No additional consent should be requested in order to process user data. Nevertheless, the data subject shall be informed that the processing of his/her personal data is a 'contractual requirement' and then obligatory, in accordance with Art 13(2)(e). In addition, the processing must be carried out in compliance with the principles and rules of the GDPR to be applied.

The latter solution is the case where the processing may be implemented even without the consent of the data subject, being

> 'necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data'.[35]

Such a balancing test should be conducted with regard to constitutional values (ie in a way that considers the right to privacy, dignity and all other personality rights) and taking into account all the circumstances surrounding the data subject's particular situation.[36]

Therefore, on the one hand, such solutions would imply that it is always possible to remedy the lack of valid consent by simply identifying a new legal ground for the processing, legitimising an uncontrolled movement of personal data, especially in online environments.[37] However, on the other hand, the viewpoint

[34] In the above case, the processing of personal data would be necessary for the *conclusion* of contract. However, in accordance with Art 6(1)(b) of the GDPR, processing is lawful if it 'is necessary for the *performance* of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract' (italic added). The overlap between these two cases may be reasonable in light of market dynamics. For a detailed analysis of this legal basis of processing, see F.G. Viterbo, n 31 above, 612-614. See also Garante per la Protezione dei Dati Personali 12 October 2004, available at www.garanteprivacy.it, where it was specified with regard to the offer of free-of-charge online services that the 'compensation' should consist in 'lawful, fair as well as proportionate user profiling', provided that no additional consent was requested to process user data, as such consent would not have been freely given. For further remarks see F.G. Viterbo, n 9 above, 230-233.

[35] Nonetheless, 'a solution that disregards the principle of consent as legitimation for data processing cannot be endorsed in the absence of a legitimate interest other than the social site operator or advertiser's need to collect personal data in order to process and sell them': C. Perlingieri, n 31 above, 77-78.

[36] Given that the courts had gone on to develop the right to confidentiality and the right to personal data protection as a constitutional check and limit on the free movement of data, this is without prejudice to the need to weigh such rights against equal-ranking interests or rights that may underpin the need for the communication or disclosure of information. For more details see the 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', adopted on 9 April 2014 by the Art 29 Data Protection Working Party.

[37] In this regard, an argument can be represented by the above mentioned Recital 24 of the Directive (EU) 2019/770 where it is specified that '[t]he personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or

that combines the presence of a fundamental right (the right to protection of personal data) as a rule with the imposition of a number of limitations to be deemed as exceptions is not adequate to the phenomenon of data protection and data flows, inasmuch as the rules applying to data processing entail some form of balancing of data subjects' and others' interests against each other. As underlined by the European Court of Justice (hereinafter: ECJ), the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society.[38]

Furthermore, the proposal for a 'ePrivacy Regulation' (replacing the ePrivacy Directive) is intended

> 'to provide a high level of protection to both content and metadata by giving consent, as defined in the GDPR, a central role for the processing of electronic communications data'.[39]

In particular, as regards the issue of 'tracking-walls' obliging the user to consent to the use of third-party tracking cookies despite these are unnecessary for the performance of the service concerned, the proposal encourages providers of software enabling access to internet and web browsers to provide easy ways for end-users to select or change the privacy settings at any time and signify their 'freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment'.[40]

Irrespective of the consent rule and the legal basis of the processing, the major challenge faced in the online world is how to ensure both compliance with data protection principles by online data controllers and the effectiveness of rights enforceable by data subjects in order to retain control over their own personal data or to prevent a breach of privacy or of dignity and autonomy.[41] The pivotal safeguard to be ensured is that both the rights of data subjects and

create with the use of the digital content or digital service. *Union law on the protection of personal data provides for an exhaustive list of legal grounds for the lawful processing of personal data*' (italics added).

[38] See Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert* v *Land Hessen*, Judgment of 9 November 2010, para 48, available at https://tinyurl.com/u5wdtpg (last visited 30 December 2019). On this assumption see also N. Witzleb et al, 'An Overview of Emerging Challenges in Privacy Law', in Ead, *Emerging Challenges in Privacy Law* (Cambridge: Cambridge University Press, 2014), 1.

[39] See EDPS, 'Opinion 6/2017' n 29 above, para 3.2.

[40] See Recital 24 of the 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2202/58/EC (Regulation on Privacy and Electronic Communications)', 10 January 2017, COM/2017/010 final - 2017/03 (COD), available at https://tinyurl.com/uc8ajkj (last visited 30 December 2019); and EDPS, 'Opinion 6/2017' n 29 above, para 3.4.

[41] On this issue see D. Korff and I. Brown, 'Comparative Study on Different Approaches to New Privacy Challenges, in particular in the light of Technological Developments. Final Report', 20 January 2010, available at https://tinyurl.com/s3amrhb (last visited 30 December 2019).

the data protection principles that are mandatory for any data controller are not dangerously reduced or weakened by the absence of supervisory authorities controls or by the courts' interpretations.

For all the measures provided by the GDPR, the starting point is focusing on the purposes of the processing. These purposes are 'the "*raison d'être*" of the processing operations'.[42] They must be 'explicit, specified and legitimate'[43] and constitute one of the parameters for assessing the lawfulness of all data processing. If the purposes of processing are sufficiently specific and clear, individuals know what to expect and transparency is enhanced. At the same time, clear delineation of the purposes is important to enable data subjects to effectively exercise their rights, such as the right to object to processing.[44]

Moreover, pursuant to Art 5(1)(b) of the GDPR, personal data collected for one or more purposes must 'not be further processed in a manner that is incompatible with those purposes'. It follows that any further processing for a *different* purpose is authorised as long as it is *not incompatible*: this needs to be assessed on a case-by-case basis, given the criteria specified by Recital 50.[45]

Accordingly, the purposes for which personal data are collected and processed are taken into account by the controller when assessing the following further requirements to be fulfilled in order to render the processing lawful:[46] a) personal data must be 'adequate, relevant and limited to what is necessary' in relation to the specified purposes; b) the specified purposes cannot be reasonably fulfilled by means other than the processing of personal data; and c) data processing may not disproportionality interfere with the interests, rights and freedoms at stake.

Just as the contract and its fundamental elements must be checked in order to verify their compliance with mandatory laws and the consistency of contractual contents with constitutional values, so too is the processing of personal data, which must be checked in order to assess the lawfulness of the operations set out by the

[42] The above wording is used in the 'Opinion 03/2013 on the purpose limitation', adopted on 2 April 2013 by the Art 29 Data Protection Working Party.

[43] Pursuant to Art 5(1)(b) ('purpose limitation') of the GDPR. For more details, see para III.1 of the 'Opinion 03/2013 on the purpose limitation' n 42 above.

[44] See para 3.2. of the 'Handbook on European data protection law', edited by European Union Agency for Fundamental Rights and Council of Europe (Luxemburg: Publications Office of EU, 2018): it is available at https://tinyurl.com/vrzrpa4 (last visited 30 December 2019).

[45] Pursuant to Recital 50 of the GDPR, 'in order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any *link* between those purposes and the purposes of the intended further processing; the *context* in which the personal data have been collected, in particular the *reasonable expectations of data subjects* based on their relationship with the controller as to their further use; the *nature of the personal data*; the *consequences* of the intended further processing for data subjects; and the *existence of appropriate safeguards* in both the original and intended further processing operations' (italics added). For more details see para III.2 of the 'Opinion 03/2013' n 42 above.

[46] Pursuant to Art 5(1)(c) ('data minimisation') of the GDPR. See para 3.3 of the 'Handbook on European data protection law' n 44 above.

controller. The checking has to be carried out ensuring that legitimate and worthy interests are realised and that the fundamental rights and freedoms at stake, which are susceptible to be injured through processing, are protected in the individual case.[47]

A similar approach should be adopted with regard to big data analytics and artificial intelligence-based applications, regardless of considerable agreement that in such areas the 'consent rule' and the 'limitation purpose principle' would fail to protect data subjects. In these cases, transparency should be ensured with the checking of the decision-making algorithm in order to assess the compliance of the decisional criteria with constitutional principles and mandatory laws.[48]

V. Analogies and Connections with Consumer Protection Directives

Given the above frame of principles enhancing the user-centric approach in data protection, the GDPR seems to outline a system of protection of data subjects that presents the following similarities and connections with the consumer protection directives:

1. The 'targeting' criterion indicated in order to define the territorial scope of data protection;

2. The specification of the principle of transparency through the provision that any information and communication be given using 'clear and plain language';

3. The fundamental role of contractual clauses and codes of conduct in order to protect the data subject (especially in the case of transfer of his/her personal data to third countries);

4. The striving for 'effective' protection of the data subject's (fundamental) rights.

Each of these measures will be analysed further in the following parts.

1. The GDPR's Territorial Scope

Since the well-known judgment of the European Court of Justice (ECJ) on the *Costeja González* v *Google Spain SL* case,[49] EU Member States have been able

[47] For further details on the checks to be carried out on contracts, see for all P. Perlingieri, ' "Controllo" e "conformazione" degli atti di autonomia negoziale' *Rassegna di diritto civile*, 204-228 (2017).

[48] The importance of prior checking on the decision-making algorithms has been demonstrated by some recent cases. An illustration is the case of Amazon, which has recently experimented with using machine learning to build a recruitment tool. The project was later abandoned after the engineers found that their artificial intelligence-based tool showed a bias against women: for more details see *Business Insider* news, available at https://tinyurl.com/smnxxmn (last visited 30 December 2019).

[49] Case C-131/12, *Google Spain SL, Google Inc.* v *Agencia Española de Protección de Datos (Aepd), M. Costeja González*, Judgment of 13 May 2014, available at www.eur-lex.europa.eu, and *Computer Law Review International,* 77 (2014). This judgment was implemented by the

to exert pressure so that their own national laws apply to the processing of personal data carried out by big online companies, such as Google and Facebook. Before this judgment, Opinions 1/2008 and 05/2009 adopted by the Data Protection Working Party[50] clarified that Directive 1995/46 generally applied to the processing of personal data by both search engines and social network service providers, although they did not have an establishment in the territory of a Member State: in this case, it was sufficient that the provider had made use of equipment, automated or otherwise, in the territory of a Member State (for example, it made use of cookies or similar software devices) for the purpose of processing personal data in order that the data protection law of that Member State be applied.

Consequently, the EU legislator has defined the territorial scope of the GDPR on the basis of two key criteria: the 'establishment' criterion as per Art 3(1) and the 'targeting' criterion as per Art 3(2).[51]

Pursuant to the former criterion, the GDPR applies to

> 'any processing of personal data *in the context of the activities of an establishment* of a controller or a processor in the Union (…) regardless of whether the processing itself takes place within the Union'.[52]

Establishment implies the effective and real exercise of activity through stable arrangements.

Pursuant to the 'targeting' criterion, the GDPR applies to

> 'the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union (…) *where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment*',[53]

which may occur, for instance, when the online service provider makes

Data Protection Authorities represented in the Data Protection Working Party (WP 29) through the publication of the following document: 'Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (Aepd) and Mario Costeja González" C-131/12', adopted on 26 November 2014. In Italy the Judgment has been followed by the 'Decision Setting Forth Measures Google Inc. is Required to Take to Bring the Processing of Personal Data under Google's New Privacy Policy into Line with the Italian Data Protection Code' adopted by Garante per la Protezione dei Dati Personali 10 July 2014, available at www.garanteprivacy.it. For more details on the issues treated by the Judgment, see F.G. Viterbo, 'The Flow of Personal Data on the Internet: The Italian and European Google Cases' 2 *The Italian Law Journal*, 327- 363 (2015).

[50] See 'Opinion 1/2008 on data protection issues related to search engines', adopted on 4 April 2008, and 'Opinion 05/2009 on online social networking', adopted on 12 June 2009, (both available at https://tinyurl.com/r7kb8dx (last visited 30 December 2019)).

[51] For further details on these two criteria see the 'Guidelines 3/2018 on the territorial scope of the GDPR' adopted by the European Data Protection Board (EDPB) on 16 November 2018, available at https://tinyurl.com/syopwfp (last visited 30 December 2019).

[52] Italics added.

[53] See Art 3(2)(a) of the GDPR. Italics added.

> 'use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language'.[54]

This provision ensures the effectiveness of data protection in the online environment, even when a service or a digital content is supplied not in exchange for a price but where the user affords access to his/her personal data. Therefore, regardless of the above-mentioned issue of identifying a legitimate basis of the processing, by way of consideration for the supply of a free online service, the consumer can allow personal data to be processed by the provider under the assurance that the processing would be carried out in compliance with the GDPR.[55] This is all the more important given that large online companies that offer online services and digital content for free have the means to make it difficult to verify the place of their establishment and to identify the applicable law.

In addition, the GDPR applies to

> 'the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union (…) when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union',

which may occur when individuals

> 'are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him'.[56]

Regardless, as a general principle, 'where the processing of personal data falls within the territorial scope of the GDPR, all provisions of the Regulation apply to such processing'. Therefore, controllers and processors, especially those offering goods and services at international level, have

> 'to undertake a careful and *in concreto* assessment of their processing activities, in order to determine whether the related processing of personal

[54] See Recital 23 of the GDPR.

[55] F.G. Viterbo, 'The Flow of Personal Data' n 49 above, 360. Moreover, in the above cases, pursuant to recital 80 and Art 27 of the GDPR – 'unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing' – 'the controller or the processor should designate a representative' on the basis of a mandate contract. Art 27(4) specifies that 'the representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing'. See also F. Pizzetti, n 20 above, 62.

[56] See Art 3(2)(b) and Recital 24 of the GDPR.

data falls under the scope of the GDPR'.[57]

Given the territorial scope of the GDPR, some authors have recognised in its measures a vocation to have a global application.[58]

It would be better to think of both the 'establishment' and 'targeting' criteria like a solution that must be endorsed due to the simple fact that they may ensure the *effectiveness* of the protection of data subjects (fundamental) rights.[59] The aim to achieve an *effective* protection has already been embraced in the area of consumer law, in accordance with Art 47 of the 'Charter of Fundamental Rights of the EU' having regard to the 'right to an effective remedy'.[60]

2. The Specification of the Principle of Transparency Through the Provision that any Information and Communication Be Given Using 'Clear and Plain Language'

Another connection with the consumer protection directives introduced by the GDPR is the specification of the principle of transparency under Recital 39 and Art 12(1). Pursuant to these provisions, the principle of transparency requires that 'any information and communication' pertaining to the processing of personal data be '*concise*', '*easily accessible* and *easy to understand*', and that '*clear and plain language*' be used, 'in particular for any information addressed specifically to a child'.[61] Moreover, 'in order to give *in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing*', the above information 'may be provided in combination with *standardised icons*',[62] even on the basis of the delegated acts to be adopted by the Commission in accordance with Art 92.

The wording of the GDPR's text brings to mind the transparency of contractual terms in consumer contracts required by Art 5 of Directive 93/13/EEC pursuant to which

> 'in the case of contracts where all or certain terms offered to the consumer

[57] 'Guidelines 3/2018' n 51 above, 4.

[58] As regards this point, in the Italian debate, see M.G. Stanzione, 'Genesi ed ambito di applicazione', in S. Sica, V. D'Antonio e G.M. Riccio eds, *La nuova disciplina europea della privacy* (Milanofiori Assago: Wolters Kluwer, 2016), 19; G. Finocchiaro, n 10 above, 19-20.

[59] On the aim to provide the data subject with effective and enforceable rights see para 5.4 below. Moreover, one must not overlook that the GDPR limits its scope to any information relating to natural persons only, without leaving any margin of discretion to Member States as regards the possibility of extending the protection to legal persons with regard to the processing data that concern them, as had been permitted by Directive 95/46. Likewise, the protection of consumers' rights is addressed to natural persons only, given that in the definition of 'consumer' given by the Directives on consumer's contracts there is no room for legal persons.

[60] For further remarks see F.G. Viterbo, *Il controllo di abusività delle clausole nei contratti bancari con i consumatori* (Napoli: Edizioni Scientifiche Italiane, 2018), 85.

[61] Italics added.

[62] Pursuant to Recital 60 and Art 12(7) of the GDPR. Italics added.

are in writing, *these terms must always be drafted in plain, intelligible language*';[63]

and by Art 13(1) of Directive 2017/14/EU pursuant to which

'*clear and comprehensible general information* about credit agreements is made available by creditors or, where applicable, by tied credit intermediaries or their appointed representatives at all times on paper or on another durable medium or in electronic form'.[64]

Therefore, in order to grasp the effective contents of the information to be provided to the data subject pursuant to Art 12(1) of the GDPR and the consequences of acknowledging the violation of the transparency obligations, one must not overlook that there is a body of case law dealing with a similar issue in the context of consumer protection that may apply by analogy.

In some well-known judgments, the ECJ has held that

'information, before concluding a contract, on the terms of the contract and the consequences of concluding it is of fundamental importance for a consumer',

insofar as it is on the basis of that information in particular that the consumer takes his/her own decisions about the contract. Accordingly,

'the requirement that a contractual term must be drafted in plain intelligible language is to be understood as requiring not only that the relevant term should be grammatically intelligible to the consumer, but also that the contract should set out transparently the specific functioning of the mechanism (…) to which the relevant term refers and the relationship between that mechanism and that provided for by other contractual terms (…), so that that consumer is in a position to evaluate, on the basis of clear, intelligible criteria, the economic consequences for him which derive from it'.[65]

[63] Italics added. In Italy, the above part of Art 5 has been implemented under Art 35(1) of the so-called 'consumer code' (decreto legislativo 6 September 2005 no 206), in order to comply with that Directive on unfair terms in consumer contracts. This is also reflected in Recital 42 of the GDPR, that specifically refers to the Directive 93/13/EEC regarding pre-formulated declarations of consent. For further remarks, see D.J.B. Svantesson, 'Enter the Quagmire – The Complicated Relationship Between Data Protection Law and Consumer Protection Law' 34 *Computer Law & Security Review*, 25-36 (2018).

[64] Italics added. In Italy, the above Art 13(1) has been implemented under Art 120-*novies*(1) of the decreto legislativo 1 September 1993 no 385 (the so-called 'Testo Unico Bancario'), in order to comply with that Directive on credit agreements for consumers relating to residential immovable property.

[65] See Case C-26/13, *Árpad Kásler* v *OTP Jelzalogbank Zrt*, Judgment of 30 April 2014, available at www.eur-lex.europa.eu, *Contratti*, 853 (2014), with the comment of S. Pagliantini,

It follows that if a contractual term does not fit such a requirement, it may be deemed unfair and not binding on the consumer as a result.

Transposing these rulings into the scope of the principle of transparency under the GDPR, it should be acknowledged that the requirement that '*clear and plain language*' be used for any information and communication pertaining to the processing of personal data is to be understood as requiring not only that the relevant information should be grammatically intelligible to the data subject, but also that all information to be provided pursuant to Arts 12, 13 and 14 should set out transparently the purposes of the processing and all other case specifications (eg whether the data subject is obligated to provide his/her personal data as well as whether the provision of personal data is a statutory or contractual requirement; the existence of automated decision-making, including profiling, as well as the logic involved; and whether personal data may be transferred to third countries or international organisations), so that data subjects be able to assess the envisaged consequences of such processing, especially in terms of concrete risks for their fundamental rights and freedoms. It is on the basis of this information, in particular, that the data subject takes his/her own decisions about the processing of personal data. It follows that if the information provided to the data subject does not fit such requirements, the processing of personal data may be considered unfair and not lawful as a consequence, especially when a ground for lawfulness is given by the data subject's informed consent. This checking must be carried out with consideration of the specific circumstances to be assessed on a case-by-case basis.

Given the aforementioned case law, the transparency of the information to be provided to the data subject pursuant to Art 12, para 1, of the GDPR can be acknowledged as a mandatory principle, binding all EU Member States irrespective of their internal data protection laws. The only cases where the scope of this mandatory principle can encounter limitations are specified by Art 23, para 1, of the GDPR. These are restrictions that can be adopted by the EU law or a Member State law as necessary and proportionate legislative measures to safeguard some important objectives of general public interest in a democratic society, as long as they do not lead to bias against the essence of the fundamental rights and freedoms involved.

3. The Fundamental Role of Contractual Clauses and Binding Corporate Rules in Order to Protect the Data Subject (Especially in the Case of Transfer of His/Her Personal Data to Third Countries)

'L'equilibrio soggettivo dello scambio (e l'integrazione) tra Corte di Giustizia, Corte costituzionale ed ABF: "il mondo di ieri" o *un trompe l'oeil* concettuale?', ibid 854-872; and Case C-92/11, *RWE Vertrieb AG* v *Verbraucherzentrale Nordrhein-Westfalen e.V*, Judgment of 21 March 2013, available at www.eur-lex.europa.eu. For further remarks on these rulings, see F.G. Viterbo, n 60 above, 65-69.

EU Member States' legislation ensure that contracts concluded with consumers do not contain unfair terms; moreover, if such terms are used regardless, they will not bind the consumer and the contract will continue to bind the parties without the unfair provisions.

In contrast, in accordance with the GDPR, the addition of particular contractual clauses or adherence to a specific code of conduct within trade agreements can serve to guarantee an adequate level of protection of personal data with respect to some particular cases of data processing. The issue of contractual protection against the risks deriving from personal data processing is destined to acquire greater importance alongside the increasing number and complexity of international transfers of personal data (resulting from, eg, cloud computing, globalisation, data centres, social networks). The principal condition for any transfer to non-EU countries is the existence of an adequate level of protection in the recipient country, a level that is assessed by the European Commission pursuant to Art 45. If a country is not found to ensure an adequate level of protection, certain contractual safeguards may serve to permit the transfer of data.

In accordance with Art 46, these safeguards may be provided for (in particular) by:

i) *Standard data protection clauses*[66] adopted by the Commission or those previously adopted by a supervisory authority and hence approved by the Commission;

ii) *Binding corporate rules* (hereinafter: BCRs)[67] stated by a corporate

[66] In order to facilitate compliance with the Directive 95/46 of data transfers outside the EU, the European Commission adopted sets of standard contractual clauses – 2001/497/EC on 15 June 2001 and 2004/915/EC on 27 December 2004 – in order to frame transfers between controllers; and 2010/87/EU on 5 February 2010 for transfers between controllers and processors. For further details, see F.G. Viterbo, *Protezione dei dati personali* n 9 above, 267-276.

[67] For further details on BCRs, see the following documents adopted by the Art 29 Data Protection Working Party: 'Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data', WP 264, 11 April 2018; 'Recommendation on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data', WP 265, 11 April 2018, both available at https://tinyurl.com/yemrwble (last visited 30 December 2019); 'Explanatory Document on the Processor Binding Corporate Rules', WP 204, 19 April 2013; 'Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules', WP 108, 14 April 2005; 'Working Document: Transfers of personal data to third countries: Applying Article 26, para 2 of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers', WP 74, 3 June 2003 (all documents between 1997 and November 2016 are available at https://tinyurl.com/azwd6hb (last visited 30 December 2019)). In the Italian literature see: G. Buttarelli, 'Il trasferimento all'estero dei dati personali', in G. Santaniello ed, *La protezione dei dati personali* (Padova: CEDAM, 2005), 265; V. D'Antonio, *Il trasferimento dei dati all'estero*, in P. Stanzione and S. Sica eds, *La nuova disciplina della privacy* (Milano: Giuffrè, 2004), 156; Ri. Imperiali and Ro. Imperiali, *Il trasferimento all'estero dei dati personali* (Milano: Giuffrè, 2003), 308; M. Bellabarba, 'Il trasferimento all'estero dei dati personali', in R. Panetta ed, *Libera circolazione e protezione dei dati personali* (Milano: Giuffrè, 2006), I, 1753; A. Putignani, 'Strutture contrattuali nella disciplina del trasferimento all'estero dei dati personali' *Contratti*, 843 (2001). For

group for its international transfers of personal data from the EU to organisations within the same corporate group as the controller, or annexed to the contract between an EU controller and processor's group, in accordance with Art 47;

iii) An approved *code of conduct*[68] pursuant to Art 40 together with some other specific measures;

iv) '*Customised*' *contractual clauses*[69] between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation, given authorisation from the competent supervisory authority.

There is no room here to analyse each of these measures. Nevertheless, it is important to note that although

> 'standard contractual clauses generally work best for linear transfers of data from point A to point B', 'their rigid structure is not well suited to the web of data transfers and onward transfers between service providers and subcontractors, which frequently occur on a fluid basis, particularly in cloud-based platforms'.[70]

A more flexible tool is provided by BCRs. Each set of BCRs needs to be tailor-made to the particular needs of a given corporation. In particular, they seem to accord with the pragmatic approach sought by multinational organisations with regard to compliance issues.[71] One of the fundamental requirements for

further remarks on Art 47 of the GDPR, see M.C. Meneghetti, 'Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali', in G. Finocchiaro ed, n 10 above, 469-475.

[68] In particular, Art 46, para 2, letter *e)* refers to 'an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights'. Furthermore, pursuant to Arts 24, para 3 and 28, para 5, adherence to approved codes of conduct as referred to in Art 40 may be used as an element by which to demonstrate that the processing meets the requirements of the GDPR, ensuring compliance with the obligations of the controller or processor.

[69] The wording 'customised clauses' is used by P. Hustinx, 'Besides Binding Corporate Rules (BCRs) and Safe Harbor, What are the Rules Governing the Transfer of Data Between Europe and the Newly Industrialised Countries?', 18 January 2012, available at https://edps.europa.eu/: 'Any controller wishing to use contractual clauses may choose between standard clauses adopted by the European Commission and other, customised clauses'.

[70] See the study led by the US Chamber of Commerce and Hunton & William LLP, 'Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity' 19-20 (2014), available at https://tinyurl.com/yzt8bxsf (last visited 30 December 2019), where it is specified that 'in practice, the requirement to negotiate and execute separate agreements with every data exporter and importer, and for every new category of data or purpose not covered by a preexisting agreement, represents a significant bureaucratic burden that may be particularly onerous for small and medium-sized enterprises'.

[71] See paras 1.2 and 1.3 of the 'Explanatory Document' n 67 above. For a practical implementation of BCRs, see Garante per la Protezione dei Dati Personali, 'Autorizzazione al trasferimento dei dati personali all'estero mediante BCR da parte di Intel corporation Italia Spa', 21 November 2013, available at www.garanteprivacy.it. Nonetheless, some concerns have

the implementation of this tool is the binding nature of rules both internally and towards the outside world (legal enforceability of the rules).[72] This implies that on the one hand the members of the corporate group or organization – as well as each employee within it – are compelled to comply with the internal rules. On the other hand, data subjects covered by the scope of the BCRs must become third party beneficiaries by means of inclusion of a 'third party beneficiary clause' within the BCRs, which must be given a binding effect either by unilateral undertakings (where possible under national law) or by contractual arrangements between the members of the corporate group. In any case, data subjects shall be entitled to enforce compliance with the rules both by lodging a complaint before the data protection authority or before the court competent for the EU controller. Therefore, BCRs have to contain contractual arrangements with protective effects in favour of third parties, ie data subjects.

4. The Aim to Provide the Data Subject with Effective and Enforceable Rights

Providing the data subject with effective and enforceable rights is pursued by the GDPR and effective protection of consumer rights is pursued by the Directives on consumer contracts.

In this regard, an illustration is given by the implementation of the GDPR measures for the transfer of personal data to third countries on the basis of appropriate safeguards or an adequacy decision.

First, the safeguards provided by BCRs must fulfil a certain level of adequacy and effectiveness. In particular, 'effectiveness' refers to the mechanisms for ensuring the verification of compliance with the BCRs (eg an audit programme), the complaint procedures to be handled by the corporate group and the mechanisms for reporting to the competent supervisory authority any legal requirements from a third country that are likely to have a substantial adverse effect on the guarantees provided by the BCRs.[73]

Second, when assessing the adequacy of the level of data protection provided by a third country or when negotiating a legally binding convention or another instrument with a third country in order to permit the transfer of personal data

been forecast for BCRs, described as ' "far too costly", "impractical" and "time-consuming" ': see 'Business without Borders' n 70 above, 24.

[72] See para 2.3 of the 'Explanatory Document' n 67 above.

[73] Pursuant to Art 47, para 2, of the GDPR. See Section 5 of the application form to be submitted by companies seeking approval of BCRs, which is entitled 'Effectiveness' in accordance with the 'Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data', WP 264, n 63 above; and Section 2 of the toolbox, describing the conditions to be met to facilitate the use of Binding Corporate Rules (BCR) for Processors, as shown by the 'Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules', WP 195, adopted on 6 June 2012.

pursuant to Art 45 of the GDPR, the Commission has to take into account numerous elements, starting from

> 'the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, (…) as well as the implementation of such legislation, data protection rules, professional rules and security measures, (…) case-law'.[74]

In particular:

- '[T]he third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union',
- '[T]he third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities', and
- '[T]he data subjects should be provided with *effective* and *enforceable rights* and *effective administrative* and *judicial redress*'.[75]

It is precisely in this respect that the US and EU should negotiate and establish a new framework ensuring an adequate level of protection for data transfers from the EU to organizations established in the US, taking into account the level of protection ensured by the GDPR, given that the 'EU-US Safe Harbor' adequacy Decision was declared invalid by the ECJ[76] and replaced by the 'EU-US Privacy Shield' adequacy Decision, adopted on 12 July 2016.[77] Privacy Shield has been under fire ever since it was negotiated by the European Commission and US Department of Commerce, and now the issue of its legality has been challenged in cases that are already pending before the ECJ.[78]

The assessment of adequacy should be extended to the entire legal system of the third country.[79] Accordingly, the obligation for Member States to ensure

[74] Pursuant to Art 45, para 2, letter *a)* of the GDPR.

[75] Pursuant to Recital 104 of the GDPR. Italics added.

[76] See Case C-362/14, *Maximillian Schrems* v *Data Protection Commissioner*, Judgment of 6 October 2015, available at https://tinyurl.com/yjre2rd7 (last visited 30 December 2019). On this judgment, in the Italian debate, see A. Mantelero, 'L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per i cittadini ed imprese?' *Contratto e impresa/ Europa*, 719-733 (2015); R. Bifulco, 'La sentenza Schrems e la costruzione del diritto europeo della privacy' *Giurisprudenza costituzionale*, 289-305 (2016).

[77] For more details on the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield, see EDPB, 'EU - U.S. Privacy Shield - Second Annual Joint Review' adopted on 22 January 2019, available at https://tinyurl.com/yzzxdpr8 (last visited 30 December 2019).

[78] It will come as no surprise that the man behind one of those cases is Maximillian Schrems, the Austrian whose case brought down Safe Harbor in 2015. As with the Safe Harbor case, the contention is that US surveillance agencies have too much unfettered access to Europeans' data: for more details see J. Baker, 'EU High Court Hearings to Determine Future of Privacy Shield, SCCs', available at https://tinyurl.com/yzz9ey5c (last visited 30 December 2019).

[79] On this point see Case C-362/14 n 76 above, paras 73 and 74. Here the Court specifies

the effectiveness of the rights that consumers derive from Directive 93/13 against the use of unfair clauses implies a requirement of judicial protection, also guaranteed by Art 47 of the Charter, which must be assured both as regards the designation of courts having jurisdiction to hear and determine actions based on EU law and as regards the definition of detailed procedural rules pertaining to such actions.[80] Moreover, as regards the principle of effectiveness, the ECJ has often emphasised that national procedural provisions must meet the condition that 'they should not in practice render impossible or excessively difficult the exercise of rights conferred by the EU legal order', and thus every case in which this threat may occur must be analysed with reference to the role of the relevant provision in the procedure, viewed as a whole, before the various national bodies. In particular, 'it is necessary to take into consideration, where relevant, the principles which lie at the basis of the national legal system'.[81]

The aim of an effective protection of fundamental rights, especially in the online world, is also pursued by providing the data subject with the right to data portability, introduced by Art 20 of the GDPR.[82] This allows for data subjects to receive the personal data that they have provided to a controller in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance. Therefore, such an important tool can facilitate switching between different service providers and be implemented by means of interoperable formats such as download tools and application programming interfaces. Some authors have stressed that

that '*it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection*. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union (…), *those means must nevertheless prove, in practice, effective* in order to ensure protection essentially equivalent to that guaranteed within the European Union' (italics added). See also F. Pizzetti, n 20 above, 81.

[80] See Case C-169/14, *Sánchez Morcillo and Abril García* v *Banco Bilbao*, Judgment of 17 July 2014, para 35, available at www.eur-lex.europa.eu. 'Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Art 47 of the Charter. The first paragraph of Art 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article': Case C-362/14 n 76 above, para 95.

[81] See Case C-169/14 n 80 above, paras 31 and 34; Case C-470/12, *Pohotovosť* v *Miroslav Vašuta*, Judgment of 27 February 2014, para 51; and Case C-415/11, *Aziz* v *Catalunyacaixa*, Judgment 14 March 2013, para 50, all available at www.eur-lex.europa.eu.

[82] Pursuant to Recital 68 of the GDPR, 'that right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties'. Furthermore, it is important to note that the right to data portability does not cover 'inferred data' and 'derived data', namely personal data that are created by a service provider (for example, algorithmic results).

> 'this may incentivize the development of user-centric platforms where all digital services shall be more interconnected and so interoperable'.[83]

It is not 'a first step to an idea of data subjects' default ownership of their personal data',[84] as it could appear in the recent case pertaining to the app 'Weople'.[85] Rather, the portability of digital services would constitute a fundamental mechanism that can foster the movement of personal data on the digital market with the safeguards provided by the GDPR that must be ensured even when the data are transferred and thereby processed on the basis of a contract.

One purpose of the GDPR is to re-balance the (contractual) relationship between data subjects (consumers) and data controllers (service providers).[86] In this perspective, the right to data portability is provided in order to avoid adverse effects to the data subject and the third parties involved, insofar as personal data must not be misused by the receiving 'new' data controller (to whom the data should be transmitted at the request of the user) in a way that could be qualified as either an unlawful processing or an unfair practice.[87] On the one hand, the 'new' data controller may not use the transmitted personal data for his/her own purposes, such as to propose marketing products and services to those third party data subjects without informing them, otherwise such processing is likely to be unlawful and unfair. On the other hand, the data controller providing an online service must not reject a data portability request on the basis of the infringement of another contractual right or only for hindrance. Such a 'lock-in' effect could be qualified as an unfair business-to-consumer commercial practice pursuant to Directive 2005/29/EC.[88]

[83] See P. De Hert et al, 'The Right to Data Portability in GDPR: Towards User-Centric Interoperability of Digital Services' *Computer Law & Security Review*, 197 (2018). In particular, they observe that 'from the *user perspective*, the impact of data portability is evident both in terms of *control* of personal data (and in general in the sense of empowerment of control rights of individuals), and in terms of a more user-centric interrelation between services. At the same time, it is a challenge to third data subjects' rights'.

[84] ibid 201.

[85] As regards this case, see Garante per la Protezione dei Dati Personali 1 August 2019, available at www.garanteprivacy.it. In short, an Italian company is indeed requesting, on behalf of data subjects, the personal data held by important business entities, in particular in the large retail sector, in order to bring them together in their own database after having provided data subjects with a compensation. Therefore, the Garante has sent a request for EDPB's opinion on this case, in particular on the issue of whether the right to data portability can or cannot be exercised by delegated powers in order to create a database for data enrichment process.

[86] For further details, see para I of the 'Guidelines on the right to data portability', WP 242 rev.01, adopted on 13 December 2016, as last revised and adopted on 5 April 2017, available at https://tinyurl.com/yg4mgmzb (last visited 30 December 2019).

[87] On this point, see para III of the 'Guidelines on the right to data portability', WP 242 rev.01 n 86 above.

[88] In the above case, Arts 2, letter *e)* and 5 of Directive 2005/29/EC concerning business-to-consumer unfair commercial practices could be applied inasmuch as the unfair rejection of the data portability request could prevent the user from taking a transactional decision that he/she would have taken otherwise. In a different context, it would be easier to switch between

One must not overlook how the protection of data subjects' rights is not only based on the rules applying to data processing, given that the principles of 'data protection by design and by default' laid down by Art 25 of the GDPR must already be applied to the activity of designing and organising the methods, tools and means used for the processing. This rationale seems to be similar to that covered by the aforementioned Directive 2005/29/EC, which introduced a control over the practices preceding the contractual agreements between business and consumers in order to make negotiations compliant with fairness rules. Therefore, the GDPR measures are intended for controllers, processors and also producers of certain technologies including software, apps and devices through which personal data are processed and that should be configured by default with limited possibilities of setting. The purpose of 'data protection by design and by default' is to intervene before personal data are processed, focusing on both the process of configuring those products and the procedure of planning the data processing, in order to create all conditions ensuring compliance with the GDPR. This further approach needs to be investigated below.

VI. The Accountability and Scalability Principles to Be Implemented by the Data Controllers and Processors: A 'Contextual' and 'Tailor-Made' Approach

The GDPR has partially changed the approach to be adopted towards personal data protection.

In essence, a radical shift in the data protection policy of major online companies and many other service providers is required by the implementation of the principles and obligations stated by Chapter IV of the GDPR, while the *notice-and-consent* paradigm is now quite marginal.

A new 'contextual' and 'tailor-made' approach is given by the 'accountability' and 'scalability' principles in accordance with Arts 5, para 2, 24, 25, 32 and 35.

1. The Accountability Principle

Art 5, para 2, expressly refers to 'Accountability' in order to sum up the responsibility of the data controller for compliance of the processing with the principles laid down by para 1 of Art 5 itself. 'Accountability' is not 'liability': this must be made clear. The latter would especially be the case where the controller or processor must give appropriate compensation to any person who has suffered material or non-material damage as a result of an infringement of the GDPR,

different service providers (eg in the context of online banking or in the case of energy suppliers in a smart grid environment). Therefore, the unfair practice is likely to materially distort the economic behaviour of consumers.

provided that the exemption from such tort liability cannot be proved.[89] In contrast, the 'accountability principle' finds its own rationale in the purpose to prevent the data processing from causing any damage to data subjects and other persons, being performed on the basis of 'appropriate technical and organisational measures', including 'appropriate data protection policies', implemented by the controller.[90] In accordance with such a distinction, 'accountability' has been correctly translated into the Italian term '*responsabilizzazione*' rather than '*responsabilità*'.[91]

Moreover, there is no room for standard measures and policies. The required 'technical and organisational measures' must be implemented by the data controller

> 'taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons'.[92]

It follows that a 'contextual' approach must be applied by controllers when setting up the data protection policy in relation to processing activities. Furthermore, the data controller must be able to demonstrate that processing is performed in accordance with the GDPR by virtue of the implemented measures. These can be reviewed and updated where necessary, in relation to further changes of the 'context' in which personal data may be processed.

Therefore, the accountability principle requires a new approach by integrating legal, technical and organisational knowledge into the following three implementation stages:[93]

i) A *preliminary assessment* of the processing and relevant risks for data subjects' rights must be carried out by the controller in order to identify the appropriate technical and organisational measures ensuring compliance with the GDPR in the individual case. This can be done on the basis of the requirements established by the GDPR and the national implementing rules, as well as of further requirements identified on a voluntary basis and aimed at increasing safeguards to a higher level of data protection;

ii) The identified appropriate *measures must be applied and implemented by taking and keeping sufficient evidence of compliance* with the GDPR;[94]

iii) The *monitoring of processing operations and relevant risks* for data

[89] On civil liability in the European context see G. Alpa, 'General Remarks on Civil Liability in the European Context' 4 *The Italian Law Journal*, 47-64 (2018).

[90] Pursuant to Art 24 of the GDPR.

[91] On this point see G. Finocchiaro, n 10 above, 14-15; E. Lucchini Guastalla, 'Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori' *Contratto e impresa*, 120-121 (2018): the author stresses that the term 'accountability' is not easy to translate into the Italian (legal) language.

[92] Pursuant to Art 24, para 1 of the GDPR. Italics added.

[93] G. Finocchiaro, n 10 above, 12-16.

[94] In this regard Art 24, para 3, specifies that 'adherence to approved codes of conduct as referred to in Art 40 or approved certification mechanisms as referred to in Art 42 may be used as an element by which to demonstrate compliance with the obligations of the controller'.

subjects' rights must be assured in order to review and update technical and organisational measures where necessary.

The aforementioned first stage preceding the processing operations has been specifically regulated by the GDPR. The standard procedure for identifying the above-mentioned 'appropriate measures' must be carried out through the following steps:

- The first step is where the controller has to ascertain whether or not a significant risk to the rights and freedoms of natural persons may occur by virtue of the processing operations to be performed;

- The second step is where it is found that the processing may entail a significant risk to the rights and freedoms of individuals. In such a case, pursuant to Recital 90 and Art 35,

> 'a *data protection impact assessment* should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk';[95]

- A further step may be the 'prior consultation', where a significant risk is indicated by the data protection impact assessment, in the absence of appropriate safeguards and security measures. In such a case, the supervisory authority

[95] Italics added. One must not overlook that Recital 91 makes an open list of cases where a data protection impact assessment should be required. In particular: 'large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity'; 'other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights'; processing of personal data 'for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures'. Another case is the 'monitoring' of 'publicly accessible areas on a large scale, especially when using optic-electronic devices'. Furthermore, a data protection impact assessment is required 'for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale'. For more details, see the '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', WP 248 rev.01, adopted on 4 April 2017 and as last revised and adopted on 4 October 2017, available at https://tinyurl.com/yg3v69cx (last visited 30 December 2019). Among scholars, see 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* (London: Springer Science & Business Media, 2012), 33-74; R. Binns, 'Data Protection Impact Assessment: a Meta-Regulatory Approach' 7(1) *International Data Privacy Law*, 22-35 (2017); A. Mantelero, 'Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventive (Artt. 32-39)', in G. Finocchiaro ed, n 10 above, 287-317.

should be consulted prior to the commencement of processing activities.[96]

In light of this stepwise approach envisaged by Chapter IV of the GDPR, it would be advisable to focus on the 'technical and organisational measures' that must be implemented by the controller 'both at the time of the determination of the means for processing and at the time of the processing itself'.[97] Such measures must be 'appropriate' and 'designed to implement data-protection principles (…) in an effective manner' in accordance with Art 25, para 1. What does this mean?

2. Attention to the Principles to Be Applied in Order to Determine the Technical Measures: Data Minimisation, Confidentiality, Integrity, Data Protection by Design and by Default

A preliminary question to be investigated is whether or not the processing of personal data is necessary with regard to the 'context' of the individual case.

If the processing of personal data is not necessary then there is no risk to the rights and freedoms of natural persons, and so there is no need for any further assessment.

In contrast, if the processing of personal data is necessary in the individual case, it must fit the principle of 'data minimisation' in accordance with Art 5, para 1, letter *c)* and the principles of adequacy and proportionality in accordance with Arts 2 and 3 of the Italian Constitution. It follows that personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they would be processed'. Otherwise the processing would be unfair and unlawful.[98]

Another principle to be applied in order to make the 'technical and organisational measures' 'appropriate' is that of 'integrity and confidentiality', ensuring adequate 'security of the personal data' and 'the ongoing confidentiality, integrity, availability and resilience of processing systems and services', in accordance with Arts 5, para 1, letter *f)* and 32. In particular, the measures must be set up in such a way as to protect personal data from change, where 'change' is deemed as pertaining to:

- The expectations of confidentiality that occurs when information intended for specific recipients reaches different recipients;
- Integrity, whenever personal data undergo mutations that alter their structure, characteristics or meaning;
- Availability, whenever a piece of information is missing due to a malfunction

[96] Pursuant to Recital 94 and Art 36, para 2 of the GDPR, the supervisory authority may, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Art 58.

[97] Pursuant to Art 25, para 1 of the GDPR; compare Art 10, paras 2 and 3 of the Convention 108.

[98] On the 'purpose' as a fundamental parameter for assessing the lawfulness of the processing operations, see para 4 above.

and accidental loss, removal, cancellation or damage.[99]

Especially in the online environment it is reasonable to assume that such technical measures should be envisaged at the time of the determination of the means for processing, otherwise they could not ensure a level of security and protection appropriate to the risk. Therefore, the GDPR has introduced two fundamental principles under Art 25 for enhancing the rights and freedoms of data subjects. The European legislator has qualified them as 'data protection by design' (commonly renamed 'privacy by design') and 'data protection by default' (commonly renamed 'privacy by default setting'), respectively.[100]

The former principle finds its basis in the idea of embedding data protection safeguards in the architecture of information systems and of other types of technology that may be used for data processing. Such a viewpoint envisages data protection in proactive rather than reactive terms, making 'privacy by design' preventive and not simply remedial.[101]

Those who develop the architecture of an information system must at an early stage assess the likely risks to the rights and freedoms of individuals from using the system itself as well as the appropriate remedies. Once this impact assessment is completed, the appropriate technical tools and measures must be included in the product design. Therefore, an *ex ante* intervention is required, taking into account that this must be related to the information system under 'front-end and back-end design'.[102] In other words, the 'design' may be defined in terms of both front-end user interface, which determines the manner in which personal data are collected by users and other user experiences regarding the privacy setting (eg notice, consent, access) are handled; and back-end

[99] On this point see G. D'Acquisto and M. Naldi, *Big Data e privacy by design. Anonimizzazione. Pseudonimizzazione. Sicurezza* (Torino: Giappichelli, 2017), 171-172.

[100] The principle of privacy by design as a conceptual business model is probably due to the work of Ann Cavoukian, the Information and Privacy Commissioner (IPC) of Ontario, Canada. In particular, she advanced the view that firms may accomplish privacy by design by practicing the following seven 'foundational' principles: 1) Proactive not Reactive; Preventative not Remedial; 2) Privacy as the Default Setting; 3) Privacy Embedded into Design; 4) Full Functionality – Positive-Sum, not Zero-Sum; 5) End-to-End Security – Full Lifecycle Protection; 6) Visibility and Transparency – Keep it Open; and 7) Respect for User Privacy -Keep it User-Centric. For further details see A. Cavoukian et al, 'Privacy by Design: Essential for Organizational Accountability and Strong Business Practices' (2010), available at https://tinyurl.com/yhxwq4ux (last visited 30 December 2019). Among the Italian scholars, see R. D'Orazio, 'Protezione dei dati *by deafault e by design*', in S. Sica et al eds, *La nuova disciplina europea della privacy* (Milano: Giuffrè, 2016), 79-110; A. Principato, 'Verso nuovi approcci alla tutela della *privacy*: *privacy by design* e *privacy by default settings*' *Contratto e impresa/Europa*, 197-229 (2015); I.S. Rubinstein, 'Regulating Privacy by Design' 26 *Berkeley Technology Law Journal*, 1409-1411 (2012); U. Pagallo, 'On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law', in S. Gutwirth et al eds, *European Data Protection: In Good Health?* (Berlin: Springer, 2012), 331-344.

[101] ibid 332-333.

[102] For a more detailed analysis see I.S. Rubenstein and N. Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' 28 *Berkeley Technology Law Journal*, 1352 (2013).

software, which is generally hidden from the user but drives the heart of any digital infrastructure including the processing of personal data.

As regards the front-end user interface, an illustration of how the 'privacy by design' principle may be implemented is provided by encrypting personal data in transit and in storage, or by making use of anonymity mechanisms that delink users from all traces of their online activity or of user-centric identity management systems that enable anonymous or pseudonymous credentials. On the other hand, appropriate back-end software should include, for instance, a mechanism ensuring the automatic erasure of personal data when the purpose of the processing has been achieved, or a user-centric privacy management system that could make it easier for users to exercise data subjects' rights.

Nevertheless, the vast majority of Internet service providers continue to collect personal information about users without deeming these measures of 'privacy by design' important. Of course, after the GDPR entered into force, with a binding effect on 'data protection by design', some measures will have to be implemented by controllers. Among the various approaches to 'privacy by design' taken by commentators and scholars, two different viewpoints seem to stand out.[103] Some stress that such a principle entails an obligation to make the digital product or the online service compliant with the GDPR by building the digital system in a manner that most legal provisions on data protection should be made preventive and automatic, hence all processing operations always meet the requirements of the GDPR automatically, regardless of individual preferences and the self-determined options available to users. Others argue that 'privacy by design' should not be implemented on the basis of 'self-enforcement technologies', but rather should be applied by making use of technologies that encourage people to pay greater attention to the business privacy policy and hence to their privacy (eg user-friendly interfaces), limit the negative effects of harmful behaviour, strengthen data subjects' rights and broaden the range of their choices. This latter interpretation seems to be preferred inasmuch as it allows data subjects to make free and informed choices with regard to their own private lives, in accordance with Arts 7 and 8 of the Charter of Fundamental Rights of the Union.

Once the design of a digital system is user-friendly, one must not overlook the issue of whether such a digital system is or is not *by default setting* arranged for collecting and processing the personal data of users. Art 25, para 2 of the GDPR provides that

> 'the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed'

[103] On this point see U. Pagallo, n 100 above, 333-334.

and in particular that

> 'such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons'.

Of course, the principle of 'data protection by default' should not be limited to overlapping with the principle of data minimisation. The rationale behind such a principle should be the notion that where a setting has already been pre-selected, users tend not to change it and instead remain on the default setting. A typical example is represented by profiling cookies, which are by default transferred to the user's terminal except when blocking them by refusing consent, but it is well-known that the vast majority of users do not block or are unable to block them. Thus, the principle of 'data protection by default' should be interpreted as entailing that, by default, the functioning of each information system or digital platform should be set up in a manner that the user's personal data remain protected in the absence of another distinct and explicit choice.[104] It follows that by default, profiling cookies should never be transferred to the user's terminal unless the user gives his/her explicit consent, or another legal basis for profiling can be found.[105]

3. The 'Scalability Principle'

The accountability principle engenders a governance model based on organisations taking responsibility for protecting privacy and information security appropriately and protecting individuals from the risks to their fundamental rights and freedoms as a consequence of data protection failures.[106] In Italy, a practical application of this model is given by the recent approval of a 'Code of Conduct' for the processing of personal data, addressed to companies that manage commercial information.[107] Pursuant to this Code, these companies may process personal data on a legal basis other than data subjects' consent, but must do so in accordance with a risk-based approach, adopting technical, procedural, physical and organisational measures in order to prevent or minimise the risks of destruction, loss, modification and unauthorised disclosure of managed personal data.

In the recent debate on Arts 24 and 25 of the GDPR, some scholars have remarked that the two articles can be read as specifying that the compliance measures taken by the controller should consider the risks posed by the processing

[104] On this point see R. D'Orazio, n 100 above, 89.

[105] This issue is presently discussed with regard to the proposal for a 'ePrivacy Regulation': see EDPS, 'Opinion 6/2017' n 29 above, para 3.5.

[106] A. Cavoukian, S. Taylor and M. Abrams, n 100 above, 407.

[107] See Garante 12 June 2019, doc. web no 9119868, available at www.garanteprivacy.it. Commercial information is a fundamental tool to evaluate the solidity and reliability of potential customers or business partners.

operations, and thus the risk-based approach should be the reference point for the interpretation and implementation of the GDPR.[108]

The Art 29 Working Party (WP29) has always supported the inclusion of a risk-based approach in the EU data protection legal framework. It is important to recall its statement of 27 February 2013 on discussions regarding the data protection reform package adopted on 2012, its view being that

> '*all obligations must be scalable to the controller and the processing operations concerned*. Compliance should never be a box-ticking exercise, but should really be about ensuring that personal data is sufficiently protected. How this is done, may differ per controller. This difference however, is not only dependent on the size of the controller, or on the amount of processing operations it carries out, but is also dependent for example on the nature of the processing and the categories of the data it processes. (…) Therefore (…) *all controllers must act in compliance with the law, though this can be done on in a scalable manner*'.[109]

The GDPR has developed the risk-based approach as previously known under the Directive 95/46/EC[110] by implementing the 'scalability' principle, that is to say the 'scalability' of compliance measures based on risk:

> 'This means that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk'.[111]

In accordance with a 'tailor-made' approach, the vast majority of technical and organisational measures to be adopted by controllers and processors may vary with regard to all of the specific circumstances in which processing is performed in the individual case, such as its 'nature' (eg large-scale processing, ie the processing of a considerable amount of personal data), 'scope' (eg processing of special categories of personal data), 'context' (eg online or offline; a big company or a small or medium-size entrepreneur as controller), 'purposes' (eg entailing

[108] See C. Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' 9(3) *European Journal of Risk Regulation*, 502-526 (2018); compare A. Mantelero, n 95 above, 306.

[109] See the 'Statement of the Working Party on the current discussions regarding the data protection reform package' adopted on 27 February 2013, available at https://tinyurl.com/yhxwq4ux (last visited 30 December 2019). Italics added.

[110] See Art 17 and recital 46 of the Directive 95/46, where it is specified that 'appropriate technical and organizational measures' must be taken in order to ensure 'an appropriate level of security, *taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing* and the nature of the data to be protected' (italics added).

[111] See the 'Statement on the role of a risk-based approach in data protection legal frameworks' adopted by the Working Party on 30 May 2014, available at https://tinyurl.com/ydsbjq75 (last visited 30 December 2019).

the transfer of personal data to third countries), 'the state of art' (in particular, for technical measures), 'the costs of implementation', as well as 'the risk of varying likelihood and severity for the rights and freedoms of natural persons'.[112]

To offer more detailed examples of where the scalability principle is applied, the following measures can be taken into consideration:

- The obligations referred to in Art 30, paras 1 and 2, binding the controller to maintain a record of processing activities under its responsibility, do not apply

> 'to an enterprise or an organisation employing fewer than two hundred and fifty persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data';[113]

- A data protection impact assessment is required, *inter alia*, in the case of

> 'processing on a large scale of special categories of data referred to in Article 9, para 1, or of personal data relating to criminal convictions and offences referred to in Article 10';[114]

- The designation of a data protection officer is required, *inter alia*, where

> 'the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale';

or where

> 'the core activities of the controller or the processor consist of processing on a large scale of special categories of data'.[115]

Furthermore, it is important to note that the technical and organisational measures implemented by the controller or processor must be taken into account when deciding whether to impose an administrative fine and the amount of the administrative fine in each individual case.[116] Given that 'Member States should implement a system which provides for *effective*, *proportionate* and *dissuasive*

[112] The above parameters are mentioned in Arts 24, para 1, 25, para 1, 32, para 1 and 35, para 1, of the GDPR.

[113] Pursuant to Art 30, para 5, of the GDPR.

[114] Pursuant to Art 35, para 3, letter *b)* of the GDPR. For more details on the cases where a data protection impact assessment is required, see n 95 above.

[115] Pursuant to Arts 9, 10 and 37, para 1, letters *b)* and *c)* of the GDPR. For more details on the cases where a data protection officer (DPO) may or must be designed, as well as on position and tasks of the DPO, see the 'Guidelines on Data Protection Officers (DPOs)', WP 243 rev.01, adopted by the Working Party on 13 December 2016 and as last revised and adopted on 5 April 2017, available at https://tinyurl.com/ye3f9gyj (last visited 30 December 2019).

[116] Pursuant to Art 83, para 2, letter *d)* of the GDPR.

penalties'[117], the GDPR is also scalable with respect to the amount of the administrative fines. In particular, as regards undertakings, the infringements of specific provisions of the GDPR may be subject to administrative fines up to a determined percentage of the total worldwide annual turnover of the preceding financial year.[118]

In essence, in order to ensure appropriate safeguards for the rights and freedoms of natural persons, the compliance measures must meet all of the mandatory principles emphasised by the GDPR: transparency, accountability, data minimisation, confidentiality, integrity, data protection by design and by default, scalability. Furthermore, the compliance measures must always be considered with respect to the specific circumstances to be assessed on a case-by-case basis, and in accordance with a *proportionality* and *reasonableness* test on the extent of the risks to the rights and freedoms at stake.[119]

A similar approach should be adopted with regard to big data analytics and artificial intelligence-based applications, regardless of considerable agreement that in such an area the 'limitation purpose principle' would fail in protecting data subjects, and the risks to the rights and freedoms of individuals may be unclear or ambiguous. Nonetheless, in these cases too, data controllers and processors must guarantee the confidentiality and security of the data and take all necessary technical and organisational measures to ensure fair processing and to prevent any undue impact.[120]

VII. The Role of Data Scientists, Scholars, Lawyers and Data Protection Supervisory Authorities

Data protection issues regarding the implementation of the GDPR encompass multiple interests and expertise and hence the coordination of multiple parties, each with their own sets of concerns, whether legal, business, engineering, marketing and policy, to name but a few.

[117] Pursuant to recital 152 of the GDPR.

[118] See Art 83, paras 4, 5 and 6 of the GDPR. These provisions can make the administrative fines effective and dissuasive against the major online companies such as Google, Facebook and Apple when operating in the EU.

[119] Pursuant to Arts 7, 8 and 52, paras 1 and 4 of the EU 'Charter of Fundamental Rights'. On the fundamental role of principles as a pivotal guidance for interpreting and applying laws and rules to the individual case, see A. Federico, 'Applicazione dei princípi generali e funzione nomofilattica' *Rassegna di diritto civile*, 797-818 (2018); P. Perlingieri, 'I princípi giuridici tra pregiudizi, diffidenza e conservatorismo' *Annali SISDIC*, 1-24 (2017); Id, 'L'interpretazione giuridica e i suoi canoni. Una lezione agli studenti della Statale di Milano' *Rassegna di diritto civile*, 405-434 (2014). For a complete analysis of the reasonableness test in the civil law, see G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile* (Napoli: Edizioni Scientifiche Italiane, 2015).

[120] See 'Annex 2: Big data and open data' of the 'Opinion 03/2013' n 42 above; and para 10 of the 'Handbook on European data protection law' n 44 above.

Only by combining the work of data scientists, scholars, lawyers and data protection supervisory authorities is it possible to implement the effective strategy envisaged by the GDPR, which is grounded on the following three pillars:

a) Data protection impact assessment and implementation of the appropriate compliance measures;

b) Cooperation both at a global level among the national supervisory authorities and at a local level among controllers, processors, data protection officers (DPOs), other experts and the competent supervisory authority; and

c) Privacy education and awareness-raising activities.

The first pillar has been widely analysed above.

As regards the second pillar, the capability and willingness of supervisory authorities to cooperate with one another and, where relevant, with the Commission and the European Data Protection Board, are central to a more holistic approach to data protection.

It appears that under Directive 95/46, cooperation between authorities was often discussed but rarely occurred in practice.[121] The GDPR has significantly enhanced such cooperation by regulating it into its Chapter VII[122] and by introducing a 'consistency mechanism' to be applied

> 'where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States'.[123]

To provide some examples, this is the case where a supervisory authority aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Art 35, para 4, or a draft code of conduct pursuant to Art 40, para 7; or aims to approve binding corporate rules within the meaning of Art 47.[124] The rationale of the 'consistency mechanism' is to ensure the consistent and uniform application of the GDPR legal framework throughout the EU.

[121] On this point see EDPS, 'Report of workshop on Privacy, Consumers, Competition and Big Data' of 2 June 2014, available at https://tinyurl.com/yfj26mrz (last visited 30 December 2019).

[122] See Art 60 of the GDPR, regulating the 'Cooperation between the lead supervisory authority and the other supervisory authorities concerned'; the subsequent Art 61, para 1, according to which '[s]upervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another'; and Art 62, para 1, focusing on the 'joint operations of supervisory authorities'.

[123] See Recital 135 and Arts 63-65 of the GDPR. In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion on the matter submitted to it. The supervisory authority takes utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision. In the latter case and in other clearly specified cases where there are conflicting views among supervisory authorities, the Board may issue a legally binding decision.

[124] Pursuant to Art 64, para 1, of the GDPR.

Following a recent trend, the national supervisory authorities for data protection, competition and communications guarantees are cooperating in order to better analyse the implications of the development of the digital economy based on the acquisition and analysis of increasingly large volumes of data, for privacy, regulation and anti-trust and consumer protection. Of course, the Italian model given by the current cooperation carried out jointly by the Garante, the AGCM and the AGCom on the basis of the 'Big Data Guidelines and policy recommendations' of July 2019[125] is a good practice to be enhanced in the near future.

Similarly, at a lower level, cooperation between controllers, processors, DPOs and the competent supervisory authority is essential to the effectiveness of data protection. There is an explicit provision in this regard under Art 31. Moreover, in some cases, the supervisory authority should be consulted by the controller prior to processing in order to provide advice on the measures to be adopted, in particular where the controller has insufficiently identified or mitigated the risk on the basis of the data protection impact assessment.[126]

In Italy, recognition of the central role of the Garante is not without justification. This authority has been assigned supervisory tasks devoted to guaranteeing the right to protection both of personal data and of those fundamental rights of the individual that can be irreparably injured by the processing of data, that is, rights to privacy, personal identity and dignity. Thus, the supervisory authorities are the guardians of those fundamental rights and freedoms.

Since its earliest years of working, the Garante has generally exercised those of its powers that are directed at interrupting unlawful conduct and prohibiting its continuation. It has frequently opted for simple measures, formally finding a violation while abdicating its institutional duty to ensure the effective protection of the fundamental rights and freedoms involved.[127] In contrast, the Garante's role must be understood as sufficiently extensive to guarantee both the formal application of the legal framework and effective protection for the rights and

[125] See 'Big Data Guidelines and policy recommendations' n 15 above.

[126] Pursuant to Art 36, paras 1 and 2 of the GDPR.

[127] Illustrative is the case in which the Garante's intervention was invoked by a famous football player following the publication of photographs of him in a public place with some friends, accompanied by vulgar expressions and suggestive comments based on double meanings related to his sex life. This data processing by a journal was deemed lawful by the Garante on the basis of the following two assumptions: (i) personal data regarding circumstances or facts disclosed by the individual directly or through his public conduct could have been processed for publication in the press; (ii) the harm to the personal sphere of the data subject did not derive from the photographs disclosed, but depended on the defamatory comments, including captions, as to which the competence to assess their compliance with law and to ascertain the damage to be compensated should have been reserved to the courts. See Garante 11 December 2000, in M. Paissan ed, *Privacy e giornalismo* (Roma: Presidenza del Consiglio dei Ministri, 2003), 193. The conclusions of this case seem incoherent. Indeed, it seems that in this case the photographs, including captions and comments, represented some personal information with an evaluative content that was not necessary for the completeness of information. Moreover, the processing should have been declared unlawful if it was likely to affect the dignity of the person concerned.

freedoms involved in the processing of personal information. To this end, the Garante may exercise its powers even when it finds that processing is unfair or unlawful owing to breaches of laws that do not pertain to the protection of personal data but that can nevertheless put a data subject's fundamental right at risk. An illustrative case is that in which the Garante stated that the processing of sensitive data (disclosing racial or ethnic origin, religious or other beliefs, health and sex life), carried out by a real estate brokerage company through their collection by customers (eg sellers, buyers, tenants, landlords) at the pre-contractual stage, was unlawful because

> 'some owners would have not liked to rent apartments and offices to homosexual or non-EU people or as, in some condos, people of Muslim faith would have not been welcome'.[128]

In this case, the purpose and methods of the processing were assessed in light of the overall legal order, and the fundamental freedoms and human rights of the persons concerned were taken into account by the Garante when drawing up its decision. More specifically, the unlawfulness of the data processing was declared on the basis of its discriminatory nature, injuring the dignity of the persons concerned, and having regard to its unlawful purpose infringing the principle of equal treatment between persons irrespective of racial or ethnic origin pursuant to Directive 2000/43/EC and Arts 2 and 3 of the Italian Constitution.

It is clear that a fundamental task of data protection authorities is

> 'to counterweigh the general power imbalance between the data controllers and data subjects, and that their role is to supplement and give more force to the early stage control by the "consumers/data subjects" and the ex-post factum control by the courts'.[129]

This is all the more important in light of the challenges of the contemporary digital age.

In addition, the GDPR has provided each national supervisory authority with another fundamental task, namely promoting 'public awareness and understanding of the risks, rules, safeguards and rights in relation to processing' and 'the awareness of controllers and processors of their obligations' under the current data protection legislation.[130] It follows that awareness-raising activities will be addressed to all people, including specific measures directed at weaker data subjects such as children, as well as at various controllers and processors such as micro-, small- and medium-sized enterprises and their employees.[131]

[128] See Garante 11 January 2007, doc web no 1381620, available at www.garanteprivacy.it.

[129] R. Gellert and S. Gutwirth, 'The legal construction of privacy and data protection' 29 *Computer Law & Security Review*, 525 (2013).

[130] Pursuant to Recital 132 and Art 57, para 1, letters *b)* and *d)* of the GDPR.

[131] See the case study of IBM Corporation in A. Cavoukian, 'Privacy by Design: From Policy to

The purpose of promoting privacy education programmes, both at a social level and at a business level, is another pillar of the new legal framework. Making people aware of the risks and their rights regarding data protection, as well as making controllers and processors aware of what is expected of them in this scope, helps build a culture that values protecting personal data and allows the dignity and fundamental rights of individuals to be fully respected.

Practice', September 2011, available at https://tinyurl.com/yha8v3x8 (last visited 30 December 2019).