virt·eu

European Commission

Project no. 732027

VIRT-EU

Values and ethics in Innovation for Responsible Technology in EUrope

Horizon 2020

ICT-35-2016
Enabling responsible ICT-related research and innovation
Start date: 1 January 2017 – Duration: 36 months

D4.1
First report - limits of GDPR and innovation Opportunities

Due date: 31.12.2017
Actual submission date: 28.12.2017

Number of pages: 50

Lead beneficiary: POLITO

Author(s): Dr Alessandro Mantelero, ShairaThobani,

Samantha Maria Esposito (Politecnico di Torino)

Project Consortium

Beneficiary no.	Beneficiary name	Short name
1 (Coordinator)	IT University of Copenhagen	ITU
2	London School of Economics	LSE
3	Uppsala Universitet	UU
4	Politecnico Di Torino	POLITO
5	Copenhagen Institute of Interaction Design	CIID
6	Open Rights Group	ORG

Dissemination Level

PU	Public	**X**
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	

Dissemination Type

R	Document, report	**X**
DEM	Demonstrator, pilot, prototype	
DEC	Websites, patent filling, videos, etc.	
O	Other	
ETHICS	Ethics requirement	

Deliverable 4.1

First Report: This report to the internal members of the consortium is the synthesis and analysis of the findings of task 4.1

Virt-EU: Values and Ethics in Responsible Technical Design in Europe

Authors:

Dr Alessandro Mantelero, ShairaThobani, Samantha Maria Esposito (Politecnico di Torino)

Executive Summary

This report summarises the main findings of Task 4.1 (M3-M12), which focuses on the approach adopted by the new General Data Protection Regulation[1] (hereinafter GDPR) and its adequacy in addressing the new challenges of big data, which represent the core of many IoT applications and related business models.

From this perspective, the research carried out by the Polytechnic University of Turin (POLITO) in the last nine months has primarily focused on how the notions of purpose limitation, data minimization, data subject's self-determination are elaborated by the EU legislator in the GDPR. In particular, in line with the main goal of the Virt-EU project, this report discuss the Data Protection Impact Assessment outlined by Article 35 of the GDPR and points out the limits of this model.

These limits concern two main aspects: the existing relationship between risk assessment and purposes of data processing, which proposes again the criticisms concerning the application of the purpose limitation principle in the big data context; the adoption of a risk-assessment procedure that does not adequately consider the ethical and social impacts of data use.

These limits confirm the need to go beyond the existing model of data protection impact assessment and to adopt a more complex process of multiple-impact assessment of the individual and collective risks related to the use of data. In this light, the last part of this report describes an initial outline of the PESIA (Privacy, Ethical and Social Impact Assessment) model, which will be further developed during the next year (Deliverable 4.3).

This report is divided in five sections. The first section is a brief introduction about risk assessment and risk management in data protection. This section does not discuss the existing Privacy Impact Assessment models, which will be examined in the context of the Deliverable 4.3 (M24) since they represent the models that can be used to outline the privacy section of the PESIA.

The second section provides a general overview of the GDPR, in order to set the regulatory scenario and provide the readers without a specific legal background the main elements of the new EU data protection framework. The third section describes how Articles 35 and 36 outline the risk assessment in the GDPR and points out the limits of this model.

Finally, the fourth section addresses the main challenges of developing the PESIA model, which concern the definition of the ethical and social values necessary to carry out the assessment. To address these challenges, the PESIA model adopts an "architecture of values" which is articulated on three different levels.

The first of them is represented by the common ethical values recognised by international charters of human rights and fundamental freedoms. The second layer

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

takes into account the context-dependent nature of the social and ethical assessment and focuses on the values and social interests of the given community. Finally, the third layer consists in a more specific set of values provided by an ad hoc committee and it concerns the specific data processing application.

The ongoing research carried out by the POLITO (Task 4.2) is investigating all these three layers, extracting from a variety of documents the social and ethical values that are taken into account in data processing. To reach this goal, POLITO team is reviewing and analysing many different legal sources. The results of this study will be presented in the next report (Deliverable 4.3, M24), since these findings will be used to describe the PESIA methodology and to shape this new model of risk assessment.

1. Introduction

Many human activities imply a risk, which can be defined as an undesirable event which may or may not occur.[2] In making choices about what risks taking, individuals and society consider the magnitude of the risk. In this regard, there are two dimensions that describe risk in quantitative terms: probability and severity. The first concerns the chance that the undesirable event will materialise, while the second concerns the size and seriousness of the consequences.

In this light, since its origins, the alternative posed by risks to human behaviour has not been a black and white decision. There is not a dualism between risk and absence of risk. Individuals should decide when the levels of risks (probability and severity) are acceptable. Walking on the street, driving a car, using a knife are all daily activities that entail potential risks, but we accept these risks since we assume to be able to control and to minimise them and as carrying out these activities we obtain other benefits. In this sense, these are acceptable risks.

Any risk management model should start from these two questions: is there any risk related to the activity we want to carry out? If there is a risk, is this risk acceptable? This because if the risk assessment shows that there is no risk at all or, on the contrary, if the level of risk is too high, there is no room for risk management. In the first case the object of risk assessment is absent, while in the second any risk management strategy is useless because we have decided that the given risk is not acceptable, therefore the potentially dangerous activity will be suspended or not carried out.

The notion of acceptable risk is not linked to a specific domain, since acceptability can be described as an individual attitude towards risk and, in this sense, it is investigated by psychologists. On the other hand, acceptability of risk may have a social relevance and an impact on societal dynamics. Therefore, it should be also examined from the sociological viewpoint. Finally, acceptability may rise moral questions and assessed from an ethical perspective. The second and the third approaches are adopted in the Virt-EU project, which focuses on the collective dimension of data use and the social and ethical impact of data processing.

Since one of the main goals of the project is to define a risk assessment procedure (Privacy, Ethical and Social Impact Assessment, PESIA), the research investigates the object of the assessment and the procedural aspects. Both these dimensions of the PESIA will be in-depth addressed in Deliverable 4.3, but it is important to highlight the basic element of risk assessment in general.

In this light, from a procedural perspective and according to the dichotomous model, two different processes are used to address the risk and to define under which conditions a risk is acceptable: risk assessment and risk management. Risk assessment is traditionally considered as a value-free process, based on the scientific evidence of the potential negative outcome. On the contrary, risk management is based on values, which drive the decision about acceptable risk.

---

[2] See Asveld L. and Roeser S. (eds.) (2009) *The Ethics of Technological Risk* (London – Sterling, VA : Earthscan, 2009), 11-23.

Nevertheless, part of the risk management doctrine has criticised this distinction and pointed out how the first stage is characterised by implicit values.[3]

The presence of reference values is even more evident in the application of risk management to data protection, where the risk assessment is clearly value-based. In this case, the assessment is not a mere scientific and objective analysis (e.g. measuring the level of pollution in the soil), but it necessarily implies a preliminary overview of the values safeguarded by law, since this is a right-based assessment and not a mere costs/benefits assessment. [4]

Regarding risk management, it is based on a rational approach, considering that a risk with a smaller expectation value in terms of probability and severity is preferred to a risk with a larger expectation value. Nevertheless, this assumption is based both on the rationality of the decision maker and on an atomistic perspective, which focuses only on a given risk and on the interests directly affected by it, without considering other concurring interests (e.g. a seismic risk is measured on the basis of its potential impact on population and buildings). On the contrary, when risk management is carried out in the legal contest, all the concurring interests should be taken in to account (e.g. data protection risk due to invasive controls, such as body scan, affects individual intimacy and social freedom, but it entails potential benefits in terms of security, which should be considered).

Risk assessment and risk management support the decision maker in understanding whether a risk is acceptable or in finding solutions to make a risk acceptable. In this regard the problem of acceptability is commonly resolved in risk management through a cost/benefit analysis.

Nevertheless, to carry out this analysis it is necessary to define what can be considered as a cost and what can be considered as a benefit with regard to a given technology and its applications. Moreover, we should decide whether all the potential benefits and costs are at the same level or there are some benefits or costs that assume a higher importance. Finally, we should consider whether the costs/benefits analysis should be only based on economic values or other kind of values should be adopted with a possible consequence on the different relevance that costs and benefits may assume.

From this perspective the mentioned right-based nature of risk assessment in data processing makes the difference. The notion of risk adopted in the GDPR focuses on “material or non-material damages” that prejudice the “rights and freedoms of natural persons” (Recital no. 75, GDPR) in a manner consistent with the mentioned rights-based approach in risk management. This approach focuses on rights protection and not on a general trade-off between risks and benefits.

While according to the risk/benefit approach the assessment should be based on the comparison between the importance of benefits and the sum of all risks, without any distinction regarding the nature of risks and benefits; the rights-based approach focuses on risk mitigation and assumes that some interests (e.g. fundamental rights) are prevailing and cannot be compared with other interests that have a lower

---

[3] See Hansson, S.O. (1998) *Setting the Limit. Occupational Health Standards and the Limits of Science* (Oxford : Orford University Press, 1998), 35-73; MacLean D. (2009), in Asveld & Roeser (n 2), 115-127.

[4] On the different classifications of risks related to privacy and data protection, see also Wright D. & Raab, C. (2014) Privacy principles, risks and harms. *Int’l. Rev. L. Comp. & Tech.*, 28(3), 277-298.

relevance. Consequently, the rights-based approach focuses on the potential prejudice to fundamental rights and suggests adequate measures to reduce this risk or, where feasible, to exclude it.

Finally, it is necessary to define which kind of risk model is more appropriate in the context of IoT applications based on big data analytics or machine learning processes. In this regard, PESIA, like PIA and DPIA, are models which seem to be closer to the so-called risk and uncertainty model rather than to the traditional risk assessment model.

In this light, the Guidelines on Big Data adopted by the Council of Europe[5] suggest the adoption of "a precautionary approach in regulating data protection in this field", due to the increasing complexity of data processing and the transformative use of data in the Big Data context.[6]

This approach is adopted when new applications of technology may produce potential risks for individuals and society, which cannot be exactly calculated or quantified in advance.[7] In this sense, the obscurity of big data uses, the uncertainty characterising the applications of data science in the field of analytics and their

---

[5] Council of Europe (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. Available at <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a> accessed 29 September 2017.

[6] See Council of Europe (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (n 5), Section IV, para 2.1. On the distinction between the precautionary approach and the precautionary principle, see Peel J. (2004). Precaution - A Matter of Principle, Approach or Process?. *Melb. J. Int. Law*, 5(2), 483 <http://www.austlii.edu.au/au/journals/MelbJlIntLaw/2004/19.html> accessed 4 February 2017 ("One way of conceptualising what might be meant by precaution as an approach […] is to say that it authorises or permits regulators to take precautionary measures in certain circumstances, without dictating a particular response in all cases. Rather than a principle creating an obligation to act to address potential harm whenever scientific uncertainty arises, an approach could give regulators greater flexibility to respond").

[7] Only few contributions in law literature take into account the application of the precautionary approach in the field of data protection, see Costa, L. (2012). Privacy and the precautionary principle' in *Comp. L. & Sec. Rev.*, 28 (1), 14–24; Gellert, R. (2015). Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law*, 5 (1), 3-19. See also Council of Europe (2005). *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*, para 10 <https://rm.coe.int/16806840ba> accessed 4 May 2017; Pieters, W. (2011). Security and Privacy in the Clouds: A Bird's Eye View. In Gutwirth, S., Poullet, Y., de Hert, P., Leenes, R. (eds.), *Computers, Privacy and Data Protection: an Element of Choice* (Dordrecht : Springer) 455 ("generalised to information technology, it can serve as a trigger for government to at last consider the social implications of IT developments. Whereas the traditional precautionary principle targets environmental sustainability, information precaution would target social sustainability"). On the precautionary approach in data protection, see also Narayanan, A., Huey, J., & Felten, E. W. (2016). A Precautionary Approach to Big Data Privacy. In S. Gutwirth, R. Leenes, & P. D. Hert (Eds.), Data Protection on the Move (Netherlands : Springer), 357-385; Raab, C. and Wright, D. (2012). Surveillance: Extending the Limits of Privacy Impact Assessment. In Wright, D. and De Hert, P. (eds), *Privacy Impact Assessment* (Dordrecht : Springer) 364; Lynskey, O. (2015). The Foundations of EU Data Protection Law (Oxford : Oxford University Press) 83; Raab, C. (2004). The future of privacy protection. *Cyber Trust & Crime Prevention Project* 15 <https://www.piawatch.eu/node/86> accessed 28 April 2017.

potentially high impact on certain essential aspects of society may warrant the adoption of a precautionary approach as the default setting.[8]

Against this background, the current models of risk assessment in data protection based on Directive 95/46/EC seem to be inadequate to address these issues. As demonstrated by the findings outlined in Deliverable 2.2[9], the regulatory framework built on top of Directive is only theoretically able to take into account the social and legal implications of data use, due to the shortcoming of its operational tools.

For this reason, the following sections investigate whether the new framework outlined by the GDPR is able to overcome these limits and offer new and stronger legal solutions. To this end, the second section provides a general overview of the GDPR, while the third and fourth sections discuss the risk assessment model adopted by the EU legislator.

2. The GDPR: an overview

European data protection law is now enshrined in Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR), which will apply starting from 25 May 2018, repealing previous Directive 95/46/EC.

The new regulation is the result of a seven-year long process to modernise the European data protection framework. In 2009, the Commission launched a review of this framework and started consultations among the general public and stakeholders in order to address the new challenges posed to privacy and data protection, on the one hand, and to the free flow of data, on the other.[10]

A first line of factors driving the regulatory innovation lies in the new risks posed by technological evolution to the rights and freedoms of individuals, with special regard to the right to privacy and data protection.[11] Behavioural advertising, the expansion of social networking sites, the development of IoT devices, for instance, allow more intrusive collection and processing of data, which can be "mined" to extract further valuable information. Cloud computing makes it easier to move enormous amounts of data from one jurisdiction to another, increasing problems related to the a-territoriality of information.

---

[8] See also Tosun, J. (2013). How the EU Handles Uncertain Risks: Understanding the Role of the Precautionary Principle. *JEPP*, 20 (10), 1517-1528 <http://www.tandfonline.com/doi/abs/10.1080/13501763.2013.834549>; Aven, T. (2011). On Different Types of Uncertainties in the Context of the Precautionary Principle. *Risk Analysis* 31(10), 1515–1525 <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2011.01612.x/abstract> accessed 8 March 2017; Stirling, A. and Gee, D. (2002). Science, precaution, and practice. *Public Health Reports* 117(6) 521–533 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1497477/> accessed 8 March 2017.

[9] See Virt-EU, Deliverable 2.2 : Report on Initial Domain Mapping and Synthesis Activities, 87-90.

[10] On the process that led to the adoption of the Commission's proposal for the GDPR, see the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012 COM(2012) 11 final, 2-5.

[11] See European Commission (2010). A comprehensive approach on personal data protection in the European Union. COM(2010) 609 final, 2-3.

To counter such risks and to better protect the data subject, her position has gradually been shaped as an autonomous fundamental right. The GDPR represents just the endpoint of this process: the Charter of Fundamental Rights of the European Union, building on the existing data protection framework and on previous European case law, already establishes the right to the protection of personal data as a fundamental right.[12]

In line with the previous Directive, the regulatory changes brought by the GDPR go in this direction, describing the protection of personal data in terms of a "right to the protection of personal data" (art. 1, para 2) and considering it as a fundamental right. Under this perspective, the goal is to strengthen individuals' rights with regard to their data and to reduce the risks posed by data processing.[13]

The right to the protection of personal data is not, however, the only right to be taken into account: the GDPR explicitly states that it is not an absolute right, but that it must be balanced against other fundamental rights, such as "the respect for private and family life, home and communication, [...] freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity" (Recital no. 4 GDPR).

The second line of factors spurring the data protection regulatory innovation consists in facilitating the flow of data across the Union.[14] The broader framework is the creation of a digital single market so as to break down barriers to cross-border online activity. An important aspect is the development of a European data economy,[15] whose value is increasingly growing.[16]

In this respect, the Directive needed to be superseded as it has been cause for fragmentation among member States' legislation on data protection. The Directive was not directly applicable, but had to be enacted by each State: this has caused different implementations of the general framework on data protection and has resulted in both legal uncertainty and burdensome procedures for businesses

---

[12] Article 8 Protection of personal data.
1. Everyone has the right to the protection of personal data concerning him or her.
2, Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by the law. Everyone as the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[13] See European Commission (2012). Executive Summary of the Impact Assessment, SEC(2012) 73 final, 4, which states that one of the main policy objectives underpinning the proposal for the GDPR is "to increase the effectiveness of the fundamental right to data protection and put individuals in control of their data". See also European Commission (n 11) 5-9.

[14] See European Commission (2012). Executive Summary of the Impact Assessment (n 13) 2, 4, which states that one of the main policy objectives underpinning the proposal for the GDPR is "to enchance the internal market dimension of data protection, by reducing fragmentation, strengthening unnecessary costs and reducing administrative burden." See also European Commission (n 11) 10-13.

[15] See European Commission (2017). Mid-Term Review on the implementation of the Digital Single Market Strategy, COM(2017) 228 final, 9-11.

[16] In 2015 the European data market (where digital data is exchanged as a result of the elaboration of raw data) was estimated in almost 60 million. If we also consider the direct, indirect and induced impacts on the economy, the overall value of the data economy was estimated in nearly 300 billion in 2016. See IDC, European Data Market SMART 2013/0063, 1 February 2017 <https://ec.europa.eu/digital-single-market/en/news/smart-20130063-study-european-data-market-and-related-services> accessed 15 November 2017.

operating across Europe.

Legal uncertainty has also affected data subjects, undermining their trust in data processing and online activities, as regards security and protection of their data and rights.[17] Moreover, market fragmentation and barriers between States do not provide enough scale for a full exploitation of the potentials given by cloud computing and big data.[18] All these factors have contributed to hindering the development of the data economy.

The leading threads of the GDPR therefore remain broadly the same as the ones underlying the Directive: enhancing data subjects' control on their data and protecting their rights, on the one hand, and fostering the free flow of data, on the other. However, the GDPR proceeds to updating and reviewing the tools necessary to reach such aims in a different economic and technological context.[19]

The innovations brought by the GDPR are therefore an answer to economic changes, one of them being the widespread establishment of global online platforms, which are usually based outside the European Union and process a large amount of data related to European citizens. A first need that the European legislator had to address was therefore the scope of application of data protection law, in order to ensure its application even if controllers are not territorially established in the Union. A first step to reach this goal consists in extending the territorial scope of European data protection law. While the material scope substantially conforms to the previous Directive[20], the GDPR aims at addressing the issue of a-territoriality of information by providing for the extra-territorial application of European data protection provisions.

The new regulation applies to the processing carried out by a controller in the context of activities carried out in an establishment situated in the Union, wherever the processing takes place. It also applies to the processing of data of data subjects who are in the Union even if the controller is not established in the Union, if the processing is related to the offering of goods and services to data subjects in the Union or if the monitoring of the data subjects' behaviors takes place within the

---

[17] As confirmed by the results of European Commission (2015). Special Eurobarometer 431, Data protection < http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf> accessed 5 December 2017.

[18] See European Commission (2015). A Digital Single Market Strategy for Europe, COM(2015) 192 final, 14.

[19] As clearly emerges from the statements of the Commission in European Commission (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2: "The current framework remains sound as far as its objectives and principles are concerned, but it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity. This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities".

[20] Under art. 2, the GDPR applies to "the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system", while it does not apply to the processing carried out by a natural person in the course of a purely personal or household activity, in the course of activities that fall outside the scope of Union law, by Member States when carrying out activities relating to common foreign and security policy, by competent authorities for the purposes of criminal law and public security.

Union.

The territorial scope of European data protection regulation is thus expanded compared to previous Directive, marking an attempt to enhance the protection accorded by European regulation. In this respect, the GDPR builds upon previous disputes regarding the level of data protection accorded by US regulation, which has not always been deemed sufficient compared to European standards.[21]

2.1 General principles and basis for processing

As the goals of data protection regulation have not substantially changed, the GDPR adopts a general approach similar to the previous Directive.

The general principles relating to the processing of personal data remain lawfulness, fairness and transparency.[22] The processing must be restricted to what is necessary to achieve the legitimate purposes for which data are collected (purpose limitation and data minimisation principles) and data must be accurate, kept to date and processed as to ensure security and confidentiality.[23]

In terms of general principles, the main change introduced by the GDPR regards the principle of accountability, meaning that the controller shall be responsible for, and be able to demonstrate compliance with data protection regulation (art. 5, para. 2.) As we shall see[24], this is not a new principle, but the GDPR gives it a prominent role and draws it in more structured manner.

As in the Directive, processing of personal data is allowed only if there is a legitimate basis for the processing, which consists in the consent of the data subject or a legitimate interest of the controller. There are also other circumstances under which processing is legitimate, as when it is necessary for the performance of a contract, for compliance with a legal obligation, for the performance of a task carried out in the public interest or to protect the vital interests of the data subject or third parties. Nevertheless, the consent of the data subject (as well as the implicit consent due to a contractual relationship) and the legitimate interest of the controller are the most used criteria in the private sector and therefore, the main legal basis for data processing in the IoT sector.

As in the Directive, the GDPR recognises a primal role to the data subject's consent, which has to be freely give, specific, informed and unambiguous.[25] However, the GDPR aims to tackle the criticalities and shortcomings emerged under the

---

[21] See European Court of Justice, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, 13 May 2014, case C-131/12; European Court of Justice, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, case C-362/14. See also the following document adopted by the Article 29 Data Protection Working Party: Letter addressed to Google regarding Google Glass, a type of wearable computing in the form of glasses, 18.06.2013; Letter from the Article 29 Working Party addressed to Google regarding the upcoming change in their privacy policy, 02.02.2012; Letters from the Article 29 Working Party addressed to search engine operators, 26.05.2010. All these documents are available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm>.

[22] On transparency, see Article 29 Data Protection Working Party (2017). Guidelines on transparency under Regulation 2016/679.

[23] See Article 5 GDPR.

[24] See below Section 2.3.

[25] See Article 29 Data Protection Working Party (2017). Guidelines on Consent under Regulation 2016/679.

application of the Directive, as consent often results in a mere formality regarding which the data subject has scarce awareness and little effective control.

In order to address such issues, the GDPR provides that consent must be given by means of a statement or a clear affirmative action, whereas under the Directive it was sufficient that consent be given unambiguously, therefore allowing to infer consent from omissive conducts. It also specifies that, to assess whether consent is freely given, utmost importance should be given to the circumstance that performance of a contract is conditional on consent to data processing. This last rule is aimed at preventing the widespread practice of providing a service (such as the access to an online service) only if the user gives consent to the processing of her data which is not necessary for the performance of the contract.

In providing these stricter requirements for consent, the European legislator has built upon the interpretation given across Europe by national data protection authorities and upon the guidelines and opinions issued by the Art. 29 Working Party, which had already warned about the risk of consent being a mere formality and suggested interpretations of the Directive to overcome such risk.[26]

Regarding consent as well, the GDPR adopts the accountability approach, in the sense that the controller shall be able to demonstrate that the data subject has consented to the processing. As mentioned, accountability is a broader principle underpinning the general framework of the GDPR, which aims to make the controller accountable for the protection of data. To such end, it is on the controller to demonstrate that she has taken all necessary measures to ensure that consent has been lawfully given. Accountability therefore encourages controllers to take practical steps to comply with data protection regulation, resulting in setting up procedures to request consent.

As in the Directive, the data controller can lawfully collect and process data without the consent of the data subject if there are other legitimate basis, the broader of which is the legitimate interest clause.[27] This clause requires a delicate balancing process between the interests of the data controller and of the data subjects, as the former justify processing only if they are not overridden by the interests and fundamental rights and freedoms of the latter. It is important to underline the complexity of such balancing, which seems to be underestimated by controllers, who increasingly look towards the legitimate interests clause as a more viable alternative compared to the data subject's consent (due to the apparent stricter limits to consent required by the GDPR.)

2.2 Rights of the data subject

The GDPR follows the general approach of the previous Directive also with regard to the rights recognised to data subjects aimed at ensuring that they do not lose control over their information.

The traditional rights accorded to data subjects are the right to be informed about the

---

[26] Article 29 Data Protection Working Party (2011). Opinion 15/2011 on the definition of consent. The Working Party has confirmed its position on consent in its recently released Guidelines on Consent under Regulation 2016/679, adopted on 28 November 2017.

[27] See Article 29 Data Protection Working Party (2014). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

processing[28], the right of access[29], the right that data be correct and complete, the right to object to the processing on grounds relating the particular situation of the data subject[30] and the right not to be subject to a decision based solely on automated processing (such as profiling without any human intervention).[31]

In addition to such rights, the GDPR introduces some new rights in favor of the data subject and new duties on the data controller.

First, if processing is based on consent only (i.e. there are no other legitimate basis for processing), the data subject has the right to withdraw consent at any time, without it being necessary any justification. The withdrawal does not affect the lawfulness of the processing carried out until that moment, but after that processing must stop.

Secondly, the data subject has the right to obtain from the controller the erasure of data if such data is not necessary according to the initial purpose of the processing, if the processing is unlawful, if the data subject has opposed to the processing or if she has withdrawn her consent.[32] During the period necessary to establish if there are legitimate grounds to erase the data, the data subject has the right to obtain from the controller the restriction of the data in question. If data is restricted, the controller is allowed to process such data only with the data subject's consent or for limited purposes (such as the defense of a legal claim, the protection of the rights of other persons or for important reasons of public interest). Moreover, if the data controller has made personal data public and the data subject asks for erasure of her data, the original controller is obliged to take reasonable steps to inform the other controllers that there is an erasure request.

Thirdly, the GDPR aims at giving the data subject more control over her information by creating the new right of data portability.[33] Under this provision, the data subject

---

[28]Whatever the legitimate basis of the data processing is, data subjects need to be informed on the categories of personal data concerned, the purposes and the legal basis of the processing, the identity and the contacts of the controller, the period of data processing, the existence of automated decision making and the recipients of the data. Data subjects must also be informed about their rights regarding their personal information.

[29]That is the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, access to such data, and information regarding such data.

[30]The data subject can always object to the processing of data for direct marketing purposes.

[31] See Article 29 Data Protection Working Party (2017). Guidelines on Automated individual decision-making and Profiling for the purpose of regulation 2016/679 <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963> accessed 5 December 2017.

[32] See Article 17 GDPR, which is titled “Rigth to erasure (‘right to be forgotten’)”. This provision can also be read under the right-to-be-forgotten debate, which was first addressed at a European level by the European Court of justice in the case European Court of Justice, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, 13 May 2014, case C-131/12, where the Court stated that individuals have the right, under certain conditions, to ask search engines to remove links with personal information about them. See also De Hert, P., Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer L. & Sec. Rev.* 32 (2), 179-194; Sartor, G. (2015). The right to be forgotten in the Draft Data Protection Regulation. *International Data Privacy Law*, 5 (1), 64–72; Zanfir, G. (2015). Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The “New Clothes” of an Old Right. In Gutwirth, S., Leenes, R., and de Hert, P. (Eds.), *Reforming European Data Protection Law "Proposal for an international taxonomy on the various"* (Dordrecht: Springer) 227–249; Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the ‘right to be forgotten’. *Computer L. & Sec. Rev.* 29 (3), 229-235.

[33] See Article 29 Data Protection Working Party (2016). Guidelines on the right to data portability

has the right to receive her data in a structured, commonly used and machine-readable format, and to transmit it to a new controller. The main purpose is to allow data users to switch between different service providers without being hindered by the impossibility to bring along their data: for instance, it could be difficult for users to change email provider if they are not able to bring along all their emails and contacts from the previous service provider. It is clear that the main goal in this case is to foster competition across the internal market and facilitate the free flow of data.[34]

2.3 Duties on the controller: the accountability principle and its application

As further discussed in the following sections,[35] the individual dimension of data protection, which results in a model based on the data subject's consent and on individual rights accorded to data subjects, is not enough to properly address the risks posed by the processing of personal data. The tools to address such risks cannot be left to individuals only. There must be some duties imposed on the controllers regardless of the exercise of individual rights, so as to ensure that the rights and interests of data subjects and the community at large are taken into account. However, considering that one of the goals is to facilitate the free flow of data, such duties should not be excessively burdensome and should be the same for all controllers operating on the internal market.

Under this perspective, the GDPR brings some innovations, aimed at rendering controllers more attentive to data protection issues.

In this light, the GDPR makes accountability a general principle. Under the GDPR controllers are responsible for taking all the necessary measures to comply with data protection rules and should be able to demonstrate that such measures have been taken.[36]

In general terms, the GDPR leaves it to the controller to decide which necessary measures to adopt, as they must be assessed depending on contingent factors that the controller can better evaluate on a case-by-case basis. However, the GDPR sets up the duties of data protection by design and by default[37], which are of the utmost importance in the IoT sector as they need to be applied by technology developers in the first place.[38]

Under data protection by design obligations, the controller must take all the necessary measures to comply with data protection rules both at the time of the determination of the means of the processing and at the time of the processing itself. This means that technologies, processes, products or systems, which are used to

---

<ec.europa.eu/newsroom/document.cfm?doc_id=45685> accssed 29 March 2017.

[34] See Article 29 Data Protection Working Party (2016). Guidelines on the right to data portability (n 33), 4.

[35] See below Section 4.1.2.

[36] The GDPR reinforces some notification duties, such as in case of data breach (which must be both notified to the supervisory authority and communicated to the data subjects involved). See Article 29 data Protection Working Party (2017). Guidelines on personal data breach notification under Regulation 2016/679.

[37] See Article 25 GDPR.

[38] See Article 29 Data Protection Working Party (2014). Opinion 8/2014 on the recent Developments on the Internet of Things.

process data, shall be designed and construed with data protection requirements in mind.[39]

Data protection by default means that controller must ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. There must therefore be initial pre-settings which limit the processing to what is strictly necessary, so that the data subject is not obliged to change settings if she wants more privacy.[40]

Always to promote compliance, the GDPR mandates that, under certain circumstances, the controller appoints a data protection officer, who shall monitor compliance with data protection regulation and act as the contact point for the supervisory authority.[41]The designation of the data protection officer is mandatory only if the controller is a public authority or body, and, for other organisations, only if they, as a core activity, monitor individuals systematically and on a large scale or process special categories of data on a large scale. Outside these cases, voluntary designation of a data protection officer is still useful as it may constitute one of those measures able to demonstrate that the controller complies with data protection regulation.

The GDPR provides for a general tool that controllers shall use to evaluate the risks of data processing and therefore assess which measures to take to address such risks. While the Directive only provided for a prior consultation with the supervisory authority, under the GDPR it is on controllers to carry out a data protection impact assessment if the processing is likely to result in a high risk to the rights and freedoms of natural persons.[42]

The data protection impact assessment is therefore aimed at identifying the risks posed by the processing and the measures necessary to address them. If, however, such risks are not sufficiently reduced by adopting the measures envisaged in the impact assessment, controllers must consult the supervisory authority, who shall suggest the necessary measures to mitigate risk and, if nonetheless the risk remains too high, shall ban the processing.

Finally, with the aim of facilitating the adoption of all necessary measures to comply with data protection regulation and demonstration of such adoption, the GDPR encourages the establishment of data protection certification mechanisms and of data protection seals and marks.[43] Certifications may be issued by bodies accredited by supervisory authorities or, in any case, on the basis of criteria set by supervisory authorities. Certifications, which are voluntary, may be used to demonstrate compliance with the GDPR, but do not, per se, exclude the controller's responsibility if, in spite of the certification, the controller does not comply with data protection

---

[39] See ENISA (2014). Privacy and Data Protection by design – from policy to engineering, December 2014; ENISA (2015). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. See also European Data Protection Supervisor (2010). Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 4-10.

[40] See European Data Protection Supervisor (n. 39), 13-18.

[41] See Article 29 Data Protection Working Party (2016). Guidelines on Data Protection Officers ('DOPs').

[42] See Article 29 Data Protection Working Party (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purpose of Regulation 2016/679, 4 April 2017, revised 4 October 2017 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44137> accessed 13 October 2017.

[43] See Articles 42, 43 GDPR.

regulation.

The adoption of certifications is a sign of the growing importance of self-regulation in the field of data protection. Another important tool in such sense is the adoption of codes of conduct, whose role is substantially increased by the GDPR to the point that they can be considered as a case of true co-regulation, in the sense that private actors are called together public bodies to draw, enact and apply data protection rules.

Under the GDPR, associations and other bodies representing categories of controllers may draft codes of conduct in order to detail some aspects of data protection regulation, and shall present them to the competent supervisory authority for approval. In order to be approved, codes shall also provide for monitoring mechanisms and shall be periodically revised. As with certifications, the adoption of codes of conduct can serve as a proof of compliance with data protection regulation.

Contrary to certifications, which have the only aim of certifying compliance, codes contain rules which specify and enact the principles and rules of the GDPR. Moreover, the Commission can also decide that certain codes have general validity across the Union.

Another application of the accountability principle can be seen in the rules regarding the transfer of data to third countries and international organisations. As with the Directive, the general principle consists in the flow of data being controlled or regulated, opposed to the free flow of data if the transfer occurs among Member States. Under the GDPR, it is up to the controller to ensure that the transfer takes place only if the level of protection guaranteed by European data protection rules is not undermined by the transfer. Moreover, the controller is also responsible that onward transfers from the third country or international organisation to another third country or international organisation do not hinder such level of protection.

The main cause which legitimates third countries transfers is an adequacy decision by the Commission. In the absence of it, the GDPR provides for other instruments that allow the transfer, such as binding corporate rules[44] (i.e. personal data protection policies adopted by a controller for transfer of data to third countries within a group of undertakings or a group of enterprises engaged in a joint economic activity), standard data protection clauses to be inserted in the transfer agreement, approved codes of conduct or certification mechanisms. All these instruments require, however, some intervention of public authorities, as they must be somehow approved by the Commission or by supervisory authorities.

Compared to the previous Directive, which allowed transfers if the controller adduced adequate safeguards such as “appropriate contractual clauses” (if there was not an adequacy decision by the Commission), the GDPR identifies specific cases in which such safeguards are ensured. Moreover, the GDPR extends the rules on transfer to third countries to transfers to international organisations as well.

[44] See Article 29 Data protection Working Party (2017). Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules. See also Article 29 Working Party. See Article 29 Data protection Working Party (2003). Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to binding Corporate Rules for international Data Transfers.

2.4 Data protection authorities and remedies

With a view to strengthening compliance with data protection rules, the GDPR reinforces the role and powers of national supervisory authorities. While in the previous Directive their duties were drawn in general terms and much was left to single member States, the GDPR contains more thorough provisions.

In order to bolster their effectiveness, there are stronger independence requirements and the GDPR expressly provides that supervisory authorities be equipped with "human, technical and financial resources, premises and infrastructures necessary for the effective performance of its tasks and exercise of its powers" (Article 52).

Moreover, supervisory authorities are given more powers, such as investigative powers (for instance, to obtain from the controller access to all information necessary for the performance of their tasks), corrective powers (for instance, to impose administrative fines), authorization and advisory powers. Previously, the endowment of such powers to supervisory authorities was up to each Member State, resulting in fragmentation and less effective protection across the Union.

The GDPR also significantly reinforces cooperation between authorities. While the previous Directive only mentioned a generic duty to cooperate and exchange relevant information, the new regulation sets up specific procedures to such end.[45] Such procedures aim at addressing the problem of fragmentation, which derives from different enforcement and interpretation of data protection rules by different authorities. This could result in legal uncertainty, thus hindering the protection of data subjects and obstructing business activities related to data.

These risks are particularly evident in case of cross border processing (i.e. the processing that affects data subjects in more than one Member State or the processing which takes place in the context of activities of a controller which is established in more than one Member State), when the problem arises of identifying the competent authority. The GDPR addresses such issue, setting forth the criteria to establish which is the competent authority (the lead supervisory authority), which is usually the authority where the controller has its main establishment.[46] However, in order to ensure cooperation and consistency, the lead supervisory authority shall cooperate with all the other supervisory authorities concerned by the processing.

This mechanism facilitates consistency of the application of data protection regulation across Europe, preventing different decisions on the same issue. It also makes it easier for data controllers to deal with data protection authorities, as they have to relate with just one of them (the leading supervisory authority) even if the processing involves different jurisdictions.

Another mechanism to ensure consistency is provided by the establishment of the European Data Protection Board, which will supersede Article 29 Working Party. The board is a body of the EU and is composed of the head of one supervisory authority of each Member State. Its duty is to ensure the consistent application of European data protection regulation through the adoption of both binding and non-binding opinions addressed to national supervisory authorities (for instance, in case of disputes between authorities) and also to the Commission.

---

[45] Articles 60-67 GDPR.

[46] See Article 29 Data Protection Working Party (2017). Guidelines for identifying a controller or processor's lead supervisory authority.

The GDPR also aims to reinforce compliance by tightening sanctions in case of infringement of data protection rules.[47] While the Directive left it to single Member States to define adequate sanctions, the GDPR identifies the cases in which administrative fines need to be provided for and sets a ceiling of 20.000.000 EUR or up to 4% of the total worldwide annual turnover. The entity of the sanctions is therefore potentially high, thus encouraging compliance.

Finally, in order to encourage individuals to exercise the remedies provided for in case of infringement of data protection regulation, the GDPR introduces the right of the data subject to mandate a non-for-profit body to lodge a complain with the supervisory authority and activate a judicial remedy on her behalf.

3.The risk in data protection: building accountability in data protection

In the European legal culture, data protection is part of the broader legal category of personality rights, which is a varying and evolving category of individual rights. These rights are strictly related to human nature and the manner in which this nature assumes relevance both for the individual in itself and for its social dimension.

There is therefore a relational component of these rights, due to the interaction between individuals in society, which represents the first rationale of these rights. Honor, name, images, private life, personal information are safeguarded not as a result of a positivistic decision of the legislator, but as a consequence of specific threats to these aspects of individual life which arise in society.

From this perspective, individual image became safeguarded by a specific right when the first portable cameras appeared, since before images were mainly reproduced in paintings and clients had control over the quality of the commissioned portraits. Similarly, the penny press and its invasive attitude[48] were the main reasons of the modern right to privacy.[49]

Data protection represents the most recent expression of this evolution and expansion of personality rights.[50] Its origin is strictly related to the computer revolution and the progressive massive digitalization of information.[51] In this sense, the first data protection regulations represented the answers given by legislators to the rising concerns of citizens about social control.[52]

---

[47] See Article 29 Data Protection Working Party (2017). Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679.
[48] See Schudson, M. (1978). *Discovering the News. A Social History of American Newspaper* (New York: Basic Books) 12-60.
[49] Warren, S.D. & Brandeis, L.D. (1880). The Right to Privacy. *Harv. L. Rev.* 4(5), 193-220.
[50] See also Schwartz, P.M. (2013). The E.U.-US Privacy Collision: A Turn to Institutions and Procedures. *Harv. L. Rev.* 126, 1966, 1969-1992.
[51] See Secretary's Advisory Committee on Automated Personal Data Systems (1973). Records, Computers and the Rights of Citizens <http://epic.org/privacy/hew1973report> accessed 27 February 2014 (“A persistent source of public concern is that the Social Security number will be used to assemble dossiers on individuals from fragments of data in widely dispersed systems”).
[52] See Brenton, M. (1964). *The Privacy Invaders* (New York: Coward-McCann); Packard, V. (1964). *The Naked Society* (New York : David McKay); Miller, A.R. (1971). *The Assault on Privacy Computers, Data Banks, Dossiers* (Ann Arbor: University of Michigan Press), chs 1 and 2. See also

The introduction of big mainframe computers gave governments[53] and big corporations the opportunity to collect and manage large amounts of personal information[54]. This concentration of information in the hands of few entities, induced by the cost of the equipment and their centralized architecture, led citizens to demand legislators to have a sort of counter-control over collected data.[55] In providing this legislative answer, the necessary interplay between legal scholars and computer scientists – which characterised this field from the very beginning – led to the adoption of a procedural approach in these regulations.

The main goal of the first generation of data protection regulations was to guarantee a safe use of personal information. This result was achieved not on the basis of a general duty of care, such as in other cases of tort laws, but by means of securing the different phases of data processing, since the collection of information to its potential communication to third parties. This was also the consequence of the mentioned procedural approach.

To reach this goal, regulations focus on the internal organization of data controllers (tasks assigned to the different figures involved in the process), data processing (data security) and the external monitoring of processing (data subject's rights of access, role of Data Protection Authorities).

In this sense, from the data subject's perspective, the notion of data protection was originally based on the idea of control over information, in line with the literature of that period.[56] Nevertheless, in this model there was no space for individual consent. Indeed, in the public context, there was no room for informational self-determination in terms of negotiation about personal information because of the public nature of data controllers and the purposes of data processing.

On the other hand, data processing operations put in place by private entities were mainly related to operative functions regarding the execution of the main companies' business activities (e.g. managing lists of suppliers or clients). Data subjects were therefore involved in a very limited way.

Finally, ordinary people had no adequate skills to understand electronic data processing, since computer science was at its dawn and developed only in scientific or professional/industrial contexts. This lack of awareness among data subjects necessarily had the consequence of excluding any regulatory model based on individual self-determination and consent.

From this perspective, a central role was played by accountability in terms of data controller's duty to put in place the adequate measures to guarantee a lawful data processing. This is evident in the first European international agreement on data

---

Bygrave, L.A. 2002. *Data Protection Law. Approaching Its Rationale, Logic and Limits* (The Hague; New York: Kluwer Law International), 107-112.

[53] See Miller (n 52) 54-67; Mayer-Schönberger, V. (1997). Generational development of data protection in Europe?. In Agre, P.E. & Rotenberg, M. (eds), Technology and privacy: The new landscape (Cambridge, MA: MIT Press 1997) 221-225.

[54] See Bennett, C.J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992) 29-33, 47.

[55] See Secretary's Advisory Committee on Automated Personal Data Systems (n 51). See also Mayer-Schönberger (n 53) 223.

[56] See Westin, A.F. (1970). Privacy and Freedom (New York : Atheneum), 158-168, 298-326; Breckenridge, A.C. (1970). *The Right to Privacy* (Lincoln : University of Nebraska Press) 1-3. See also Solove, D.J. (2008). *Understanding Privacy* (Cambridge, MA : Harvard University Press) 4-5.

protection, Convention 108 adopted in 1981 by the Council of Europe, which has been the reference framework for the European legislators until the adoption of the EU Data Protection directive.

Convention 108 defines the role of the data controller ("controller of the file") and its tasks,[57] as well as it introduces specific standards in terms of data quality[58] and data security,[59] which focus on the processing operations, in line with the mentioned procedural approach, with regard to data subjects, the Convention grants individuals the rights to access data bases.[60]

This model of accountability, focused on a regulated data flow and a certain level of transparency of data processing, has been maintained over the years and is still part of the new GDPR framework.[61] Nevertheless, the technological and socioeconomic scenario of the mid 1970s has been progressively replaced by a society whose members have an increased level of digital skills and ability to use and understand computers, which in the 1980s have become largely common in companies, offices and homes. Moreover, the new marketing strategies based on electronic data processing[62] recognised an economic and bargaining value[63] to personal information.[64]

[57] According to Article 2.d of Convention 108, the controller of the file is "means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them".

[58] See Article 5 of Convention 108 ("Personal data undergoing automatic processing shall be:
a obtained and processed fairly and lawfully;
b stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c adequate, relevant and not excessive in relation to the purposes for which they are stored;
d accurate and, where necessary, kept up to date;
e preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored").

[59] See Article 7 of Convention 108 on data security ("Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination").

[60] See Article 8 of Convention 108 ("Any person shall be enabled:
a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
b to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
c to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;
d to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.")

[61] See Articles 6, 24, 28 GDPR.

[62] Although direct marketing has its roots in mail order services, which were based on personalized letter (e.g. using the name and surname of addressees) and general group profiling (e.g. using census information to group addressees in social and economic classes), the use of computer equipment increased the level of manipulation of consumer information and generated detailed consumer's profiles. See Petrison, L.A., Blattberg, R.C., and Wang, P. (1997). Database Marketing. Past, Present, and Future. *J. Direct Marketing* 11 (4), 109, 115-119 ("During the decade, companies not only learned their customer's names and addresses, they also began to collect detailed personal and purchasing information, thereby beginning to understand them as individuals rather than as part of a traditional mass audience"); Daniel, J.S. (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stan. L. Rev.* 53(6), 1393, 1405-1407.

However, a greater awareness among users regarding the electronic processing of information and the use of customers profiling for economic purposes induced a different approach to accountability. While the regulations adopted during the 1990s maintained the previous accountability tools (i.e. internal data processing organization,[65] DPAs supervision and access rights), the new role recognised to data subject's consent[66] puts on data subject's shoulders the burden to self-assess the consequences of data use.

On the one hand, this was the due acknowledgment of the central role of self-determination in managing an important element of personality and individual life (i.e. information). On the other hand, this emphasis on individual decisions made it possible to transform accountability in terms and conditions. This implied a paradox: contractual clauses made it possible to exploit personal data in a non-accountable manner on the basis of an assumed data subject's self-determination.

This idea to shift from a model based on third-party accountability towards a model more and more focused on data subject's evaluation of the consequences of data processing has shown its limits gradually and progressively, due to the increasing complexity of data analysis, which became evident with the big data revolution in the last decade.[67] The result of this further change of digital paradigm is an increasing concentration of information in the hands of a few entities and an asymmetric awareness about data use.

The role played by specific subjects in the generation or intermediation of data flows is the main reason for this concentration. Governments and big private companies (e.g. large retailers, telecommunication companies, etc.) as well as data brokers, online intermediaries and platforms process huge amounts of data while performing their daily activities. These entities have also the economic resources to invest in powerful data analytics and to recruit the best data scientists to extract predictive knowledge from this large amount of data.[68]

This digital environment is completely different from the scenario existing in the early 1990s, when the Directive 95/46/EC was discussed and then approved. In the big data context, the idea of data subject's empowerment becomes harder to be put in practice. While supermarket customers in 1990s were aware of the fact that their fidelity cards traced the list of things they bought and provided a discount on the

---

[63] The new forms of marketing were based on customer profiling and required extensive data collection to apply data mining software. The main purpose of profiling was to suggest a suitable commercial proposal to any single consumer.

[64]This process of economic exploitation of an attribute of individual personality is not new and had already affected the right to image and the right to privacy. See also Barbas, S. (2015). *Laws of image : privacy and publicity in America* (Stanford, CA : Stanford Law Books).

[65] See Article 6.2 Directive 95/46/EC.

[66]See Article 7.a Directive 95/46/EC

[67] See Bollier, D. 2010. The Promise and Perils of Big Data. Aspen Institute, Communications and Society Program ttp://www.aspeninstitute.org/sites/default/files/content/docs/pubs/The_Promise_and_Peril_of_Big_Data.pdf> accessed 27 February 2014; Mayer-Schönberger, V. & Cukier, K. (2013). *Big Data. A Revolution That Will Transform How We Live, Work and Think* (London : John Murray).

[68] See Bollier (n 67) 13 ("As a large mass of raw information, Big Data is not self-explanatory"); Boyd, D. and Crawford, K. (2012). Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly. *Inf., Comm. & Soc.*, 15(5), 666-668. See also Cohen, J.E. (2013). What Privacy is For. *Harv. L. Rev.* 126, 1904, 1924-1925; The White House (2014). Executive Office of the President. Big Data: Seizing Opportunities, Preserving Values, 7.

basis of the quantity or quality of bought items, now the same costumers are not aware that this information is used to predict their health conditions or creditworthiness. Moreover, even if they were aware of this potential use of data, they would not be able to understand the manner in which these purposes are achieved, due to the complexity of data processing, the lack of transparency and the limits which anyway necessarily affect any form of disclosure of the logic of algorithms.[69]

All these elements, here briefly mentioned, lead rule makers to reconsider the role of third-party accountability against the importance of data subject's self-assessment. Since this new environment resembles the origins of data processing, when, in the mainframe era, technologies were held by a few entities and data processing was too complex to be understood by data subjects, it is not a case that data controller accountability becomes relevant again.

In this light, Regulation 2016/679 embraces the models of privacy impact assessment that have been developed over the years in several countries and the EU legislator adopts an approach more focused on risks management rather than on mere individual self-assessment of the consequences of data processing.[70] Mapping data processing, making a formal data protection impact assessment in presence of high risks for individual rights, prior consultation of data protection authorities and the possible adoption of standards to prevent and manage the risk concerning data processing are the new tools provided by the EU legislator.[71] These new

---

[69] See also Edwards, L., & Veale, M. (2017). Slave to the Algorithm? Why a 'Right to Explanation' is Probably Not the Remedy You are Looking for (SSRN Scholarly Paper No. ID 2972855). Rochester, NY: Social Science Research Network <https://papers.ssrn.com/abstract=2972855> accessed 15 November 2017.

[70] See Article 29 Data protection Working Party (2017). 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 (n 42). See also CNIL (2015). Privacy Impact Assessment (PIA). Methodology (how to carry out a PIA) <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf> accessed 25 February 2017; CNIL (2015). Privacy Impact Assessment (PIA). Tools (templates and knowledge bases) <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf> accessed 25 February 2017; CNIL (2012). Measures for the privacy risk treatment <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf> accessed 25 February 2017; Article 29 Data Protection Working Party (2014). Statement on the role of a risk-based approach in data protection legal frameworks <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> accessed 27 February 2017; Article 29 Data Protection Working Party (2013). Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart GridTask For <http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-ecommendation/files/2013/wp209_en.pdf> accessed 27 February 2017; Article 29 Data Protection Working Party (20111). Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf> accessed 27 February 2017; Trilateral Research & Consulting (2013). Privacy impact assessment and risk management. Report for the Information Commissioner's Office prepared by Trilateral Research & Consulting <https://ico.org.uk/media/1042196/trilateral-full-report.pdf> accessed 25 February 2017. See also Vedder, A. & Naudts, L. (2017). Accountability for the use of algorithms in a big data environment. *International Review of Law, Computers & Technology* 31 (29), 206-224; Böröcz, I. (2016). Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras. *European Data Protection Law Review* 2(4), 467-480.

[71] See Articles 30, 32, 35 and 36 GDPR.

requirements complement and strengthen the original accountability measures defined in the 1970s and 1980s.

Nowadays, the complexity of data processing and its risks cannot be adequately addressed only by means of the task distribution with regard to the processing operations or the access rights, but accountability should be based on an in-depth analysis which outlines the potential negative outcomes of data use.

3.1The model of risk-assessment adopted by the GDPR

The GDPR introduces a general obligation to assess in a formal manner the risk concerning data processing. Nevertheless, the EU legislator neither imposes a formal impact assessment applicable to any kind of processing, nor defines specific mandatory standards to carry out this assessment.

Articles 24, 32, 35 and 36 of the GDPR outline a risk management model based on three different and scalable modules, from a less structured assessment to a broad in-depth analysis, which may also involve the Supervisory Authorities' prior consultation. A first by default and not formal assessment is required for all the processing operations and is a consequence of the general accountability of data controller. In this light, Article 24.1 states that the controller must implement "appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation". This obligation is more specifically defined with regard to data security, requiring data controller to take all necessary technical and organisational measures to protect data subjects, considering the severity and likelihood of the risks to fundamental rights and freedoms (Article 32).[72]

These general obligations clearly point out two fundamental elements that characterise risk assessment in the GDPR: the rights-based approach and the proportionality of the measures adopted to tackle the risks.

3.2.1 The rights-based approach and the proportionality of countermeasures

Regarding the manner in which impact assessment can be carried out, two different models are theoretically possible: the risk-based approach and the rights-based approach. In both cases, risk assessment is a value-based judgement, but the values driving the assessment are different. The first is a traditional risk/benefit analysis which looks at a prognostic balance between risks and benefits, estimated on the basis of the possible impact of the examined activities. Thus, the different interests involved are often placed on the same level.

On the other hand, the rights-based approach adopts a perspective primarily oriented towards risk mitigation and assumes that some interests (e.g. fundamental rights) always prevail and cannot be weighed against other interests of a lower order.

[72] See also Recital n. 83.

It focuses on rights protection and not on an overall trade-off between risks and benefits.[73]

It is this rights-based approach that has been adopted by the EU legislator in the field of data protection.[74] Consequently, an important feature of risk analysis in this context concerns the nature of the interests involved and identifying the importance of the risks. Risk analysis in the use of personal data is characterised by the presence of a hierarchy of potentially opposing interests and rights.[75]

From this standpoint, prejudicing the right to personal data protection cannot be justified, except by appealing to other interests or rights and on the basis of a balancing test. In line with this approach, Article 35 focuses on the risks "to the rights and freedoms of natural persons". It implies that data controllers should carry out the risk assessment bearing in mind the different nature of the rights and after conducting a balancing test.[76]

Risk analysis is not an alternative to well-established data protection rights and principles.[77] Rather, it complements them by addressing any potential prejudice with specific remedies. In this vein, the Article 29 Data Protection Working Party defined risk assessment as a "scalable and proportionate approach to compliance".[78] This means that a low risk should be considered too, but the (low) severity of this risk simplifies its assessment and mitigation.

Regarding the second character of the risk assessment, i.e. the proportionality of the measures to be adopted to tackle the risks, it is necessary to combine effective countermeasures with sustainability and affordability. In this respect, Directive

---

[73] On the different classifications of risks related to privacy and data protection, see also Wright & Raab (n 4); Moerel, L. (2014). Big Data Protection, How to Make the Draft EU Regulation on Data Protection Future Proof. Oratie Universiteit Tilburg <http://www.mondaq.com/x/298416/data+protection/Big+Data+Protection+How+To+Make+The+Draft+EU+Regulation+On+Data+Protection+Future+Proof> accessed 15 January 2017; Gellert, R. (2016). We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection. *European Data Protection Law Review* 2(4), 481 – 492.

[74] See Article 29 Data Protection Working Party (2014). Statement on the role of a risk-based approach in data protection legal frameworks (n 70).

[75] From this perspective, the risk assessment in GDPR goes beyond a narrow "harm-based-approach"; see e.g. Cate, F.H. and Mayer-Schönberger, V. (2013). *Data Use and Impact. Global Workshop* (The Center for Information Policy Research and The Center for Applied Cybersecurity Research, Indiana University) <http://info.law.indiana.edu/releases/iu/2013/12/data-use-and-impact.shtm> accessed 23 March 2017. This different approach focuses on damages (harm) and takes into consideration every potential as well as actual adverse effect, assessed on a potentially very wide scale ranging from an impact on the data subject to a general societal impact.

[76] See European Court of Justice, 13 May 2014, Case 131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, paras 80-81 ("Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C 509/09 and C 161/10 eDate Advertising and Others EU:C:2011:685, paragraph 45). In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing").

[77] See Article 29 Data Protection Working Party (2014). Statement on the role of a risk-based approach in data protection legal frameworks (n 70) 2..

[78] Ibid.

95/46/EC[79] recognises that the level of protection afforded by the risk measures should provide an "appropriate" level of security, bearing in mind the state-of-the-art and the implementation costs. Similarly, the GDPR explicitly considers the "costs of implementation" as a parameter which should be taken into account when assessing the appropriate measures to be adopted.[80]

3.2.2Derivative nature of risk analysis

The derivative nature of risk analysis originates from the fact that the adopted models of risk assessment were not developed in the field of data protection, but are specific applications in this context of principles and solutions developed over time in the area of risk management studies. These studies have come about in the years following the industrialisation of production processes, as a response to the criticalities of the so-called risk society.

Legal doctrine since the 1970s has shown great sensitivity to the role of risk management, with particular reference to tort liability and consumer protection. Outside the legal debate, risk analysis has, however, assumed the nature of process management. In this light, it has been applied to information processing and data protection, adopting models that are already known and commonly used. Thus, apart from the rights-based approach to data processing risk analysis, in the remaining aspects, the models used to conduct the assessment follow general risk management criteria.

In this light, several models of risk assessment concerning data protection and privacy have been developed over the years,[81] but they usually follow a circular model, according to the general theory of risk management. Thus, the assessment process can be divided into four separate stages: 1) identification of risks, 2) analysis of the potential impact of these risks, 3) selection and implementation of the measures to prevent or mitigate the risks, 4) regular review of the effectiveness of the measures.

These different stages are now present in the formal procedure of risk assessment required in the case mentioned in Article 35 GDPR. In this sense, Article 35.7 outlines the main elements of this assessment in a manner consistent with the commonly used models of risk analysis, which require an overview of the possible negative outcomes of the examined process or product and the subsequent identification of adequate measures to avoid or reduce these outcomes.

The adoption of a risk management approach in data protection should necessarily be coordinated with the procedural provisions that characterise this kind of regulations, respecting the principles concerning lawful data processing (Article 5). For instance, data controllers should first design their processing models in compliance with the purpose limitation and minimisation principles and then assess

---

[79] See Recital 46 and Article 17.1. Since the adoption of Directive 95/46/EC, the question of the costs of data protection has sparked a wide debate and has found an operational response in the principle of proportionality. See also Article 29 Data Protection Working Party (n 16), which has correctly pointed out the scalability of legal obligations based on risk assessment models, concluding 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".

[80] See Article 32 GDPR. See also Article 25 on data protection by design and by default, and Recitals n. 83, 84, 94.

[81] See Wright, D. and De Hert, P. (eds) (2012). Privacy Impact Assessment (Dordrecht : Springer).

the potential risks for individual rights and freedoms. Consequently, if data processing is unnecessary or disproportionate, it is not necessary to conduct a risk analysis, since it is in itself and from the outset inconsistent with its purposes.

3.3.1 The assessment procedure in the GDPR

According to general risk theory, risk is seen as an undesirable occurrence deriving from a variety of sources, such as negligent or fraudulent behaviour by data processing agents, or an external attack on computer systems. It exploits the vulnerabilities of the system – either structural (e.g. lack of software updates) or organisational (e.g. lack of awareness on the part of the controller or those responsible for the processing) – and creates a threat to the data processing.

There are therefore two components of risk: the likelihood that it will occur and the severity of its effects. Likelihood depends on the nature of the sources of risk and the vulnerabilities of the system, while severity regards the nature and the amount of information potentially concerned, as well as the number of subjects potentially exposed.

Adequate risk management measures should be taken to reduce or exclude the severity and likelihood of potential risks.[82] If both severity and likelihood are high, process/product design solutions must be introduced to reduce both. Where the risk characteristics are asymmetric (e.g. low probability combined with high severity), remedies should only focus on one of these parameters.

This tendency of risk management models to set qualitative (high, medium, low) thresholds to define the magnitude of risk and its parameters is confirmed by Regulation 2016/679. In this sense, the scalable model defined by the Regulation has its threshold in the notion of “high risk” to the rights and freedoms of natural persons. Below this threshold, the controller has to adopt “appropriate technical and organisational measures” to address the potential risk to the rights and freedoms of natural persons and review and update these measures where necessary (Article 24.1), but it is not required to carry out a formal procedure of impact assessment. By design solution, as well as any other solution to minimize the impact of data use on individual rights and freedom (e.g. pseudonimization, anonymization, limits to data retention) are therefore adopted, but without a specific and documented risk assessment.[83]

This general duty of accountability becomes stronger where the risk is high, since in these cases (Article 35) a deeper level of risk analysis is required by the GDPR, following a specific procedure, defined by this article. In this light, the definition of the level of severity and the likelihood of potential risks represent a crucial aspect in defining the applicable procedure of assessment.

Unfortunately, the GDPR does not provide a clear definition of “high risk” or a list of parameters to use in order to assess the risk level. This is consistent with the specific nature of risk assessment in the context of data protection, which is a rights-

[82] See Hansson, S.O. (2009). An Agenda for the Ethics of Risk. In Asveld, L. and Roeser, S. (2009) *The Ethics of Technological Risk* (Earthscan: London-Sterling, VA). 13
[83] See also art. 32 GDPR.

based assessment[84] focused on the rights and freedoms of the data subject. Risk should therefore be evaluated on a case by case basis and entails a balancing test of these rights and freedoms.

Notwithstanding these limits, Article 35.3 outlines three cases in which a high degree of risk in data processing is presumed and, therefore, assessment is mandatory. Moreover, the Article 29 Data Protection Working Party has recently adopted specific guidelines concerning the DPIA, which provide further clarifications and also provide a more detailed list of cases in which a high risk for individual rights and freedom may be present.[85]

The first case of high risk mentioned in Article 35.3 concerns the "systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person"[86] (e.g. the processing may lead to exclusion or discrimination against individuals).[87] According to Article 29 Data Protection Working Party, this provision refers to evaluations including profiling and decisions which are "based" on automated processing, rather than solely automated processing.[88] In this sense, Article 35(3) (a) concerns the case of decision-making "including profiling with legal or similarly significant effects that is not wholly automated, as well as solely automated decision-making defined in Article 22(1)".[89]

Regarding the evaluations and decisions based on automated processing in which a human decision-maker may play a role, some safeguards which have been suggested by the Article 29 Working Party with regard to automated processing in general can also be applicable in this case. In this sense, the Working Party provides for a list of different remedies, such as information to data subjects about the existence and logic of the automated decision-making process, explanation of the significance and envisaged consequences of data processing; data subject's right to oppose the decision or to express their point of view; algorithmic auditing; ethical review boards.[90]

The other two cases in which Article 35.3 assumes high risk concern large scale data processing. In the first case, large-scale processing regards special categories of data (sensitive data[91]) or personal information relating to criminal convictions and

[84] See also Recital n. 76.
[85] See Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (n 31).
[86] Article 35(3) (a) GDPR.
[87] See also recitals 71 and 91.
[88] See Article 22.
[89] See Article 29 Data Protection Working Party, (n. 31), 2017, 27. According to Article 29 Data Protection Working Party, (n. 42), 2017, 8, these operations include, for example, "a bank that screens its customers against a credit reference database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website".
[90] See Article 29 Data Protection Working Party (2017). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (n 31), 27 and Annex 1.
[91] See Article 9.1.

offences,[92] while the second case regards the large-scale extension of systematic monitoring of publicly accessible areas.[93]

There is a degree of uncertainty around the use of the quite vague notion of "large-scale". Recital 91 states that large-scale data processing operations are those "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". However, this clarification does not eliminate all doubts, since it is unknown when, in general terms, a certain amount of data may be "considerable". Similarly, the adoption of a territorial dimension to qualify processing ("regional, national or supranational level") is not appropriate for forms of data processing that are often independent from a territorial context, such as cloud environments with a special geometry which continuously varies.

However, the list of cases specified in the mentioned Article is not closed, since the authorities may add further cases, consistent with the room for manoeuvre which the Regulation allows to national authorities and legislators. Moreover, according to Article 35.5, supervisory authorities may also establish a list of processing operations for which no data protection impact assessment is required. In this case, the list should be made public and communicated to the European Data Protection Board.[94]

Some doubts arise about the cases in which "high risk" can be excluded by the Supervisory Authorities. There are difficulties in listing the circumstances in which a risk of prejudice to individual rights and freedoms can be excluded.[95] As a default rule, the European data protection authorities have concluded that "in cases where it is not clear whether a DPIA is required, the Article 29 Working Party recommends that a DPIA be carried out in any case, since a DPIA is a useful tool to help data controllers comply with data protection law". This default approach is in line with the rights-based approach adopted by the EU legislator in the field of data protection.

In general, the GDPR highlights the relation between potential high risks and the use of new technologies, both in terms of new technological solutions (e.g. assistive robots, self-driving cars) as well as for new forms of data processing (e.g. big data[96]). In this sense, Recital 89 states that processing operations which are likely to result in a high risk to the rights and freedoms of natural persons "may be those which, in particular, involve using new technologies, or are of a new kind".

---

[92] See Article 10.

[93] See also Article 29 Data Protection Working Party (n 42) 8 ("This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s)").

[94] When one of these lists, which extend or restrict the cases of mandatory DPIA, involve "processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union" the competent supervisory authority should previously apply the consistency mechanism referred to in Article 63 GDPR. See Article 35.6.

[95] There is a tension between this general *a priori* assessment, which excludes high risks, and the notion of risk analysis itself. The latter necessarily focuses on the specificity of the concrete case, making it hard to assume that some kinds of data processing are per se without a high risk. Indeed, the particular nature of a given use of data may argue against such a presumption, bearing in mind that personal and sensitive data may be inferred from non-personal or non-sensitive information.

[96] See Article 35.3.a.

Based on the wording of the GDPR, the various elements used to describe the cases in which a DPIA is required remain uncertain. Consequently, the Article 29 Working Party has recently adopted specific guidelines on DPIA. These guidelines not only clarify the provisions of the Regulation, but also provide a broader interpretation of the cases in which the high risk is presumed. With regard to the use of data for evaluation or scoring purposes,[97] the Working Party seems to suggest a broader reading based on the reference to decisions that produce legal effects concerning the natural person "or similarly significantly affect the natural person", which is interpreted as encompassing any data processing which may lead to exclusion or discrimination against individuals.

This approach in favour of a broader interpretation of the provisions of the Regulation is even more evident with regard to sensitive data. According to the Article 29 Working Party, this category includes information that is not necessarily sensitive, but "may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud)".

Similarly, the definition of "large scale" is interpreted by the Working Party in such a way as to give more safeguards to data subjects. For instance, the Working Party classifies hospital information systems (with no distinction in terms of size of hospital) as large-scale processing and excludes only processing of sensitive data by a medical doctor in a one-person practice.[98]

The Working Party guidelines also reduce the degree of uncertainty concerning the "large scale" notion, giving some indications about the factors to be considered when assessing whether data processing is on a large scale. These are: a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b. the volume of data and/or range of different data items being processed; c. the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity.

Finally, the Working Party outlines new cases in which the DPIA is required, which are not listed in Article 35.3 but which are considered high-risk. According to Article 35(4), this list should be adopted at a national level by supervisory authorities. These new cases are based on broader categories, such as the notions of reasonable expectation of data subjects,[99] vulnerable data subjects (e.g. employees, children, mentally ill persons, asylum seekers, elderly people, patients)[100], innovative use or applying technological or organisational solutions[101]. However, there are cases in

---

[97] Art. 35.3.a ("a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person").

[98] See Article 29 Data Protection Working Party (n 42) 8, 10.

[99] See Article 29 Data Protection Working Party (n 42) 9 ("Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject"). Regarding the notion of reasonable expectation, see also Recitals no. 47 and 50.

[100] Ibid ("the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data").

[101] See also Article 35(1) and Recitals no. 89 and 91. See Article 29 Data Protection Working Party (n 42) 9 ("the use of such technology can involve novel forms of data collection and usage, possibly with

which a potential high risk is assumed because of the specific nature of processing, such as data transfer across borders outside the European Union[102] or data processing which in itself "prevents data subjects from exercising a right or using a service or a contract".[103] In all these cases, the use of these broader notions significantly increases the application of Article 35 and extends the cases of mandatory adoption of DPIA.

3.3.2 The DPIA procedure in an organisational perspective

From an organisational perspective, the DPIA is a procedure which should not be necessarily conducted for all the data processing operations which are likely to result in a high risk, since a single assessment may address a set of processing operations that present similar high risks.[104] This means that data controllers should firstly conduct an overview of the processing operations[105] to identify those which show similar risks. On the basis of this aggregation of processes, a data controller can use a single DPIA to assess all the processing operations which present risks classified as high by Article 35.

Moreover, as suggested by the Article 29 Working Party, where similar technology is used to collect the same sort of data for the same purposes, different controllers may carry out a single DPIA covering the processing by these separate controllers (e.g. a network of municipal authorities that are each setting up a similar CCTV system).[106]

This last scenario, involving different parties, may be characterised by a higher level of interplay between data controllers, who – in certain circumstances –, can also act as joint-controllers (Article 26). In this case, to better manage controllers' responsibilities, a clear definition of their different obligations would also be valuable for the risk assessment and DPIA. In this way, it is possible to define which party is responsible for which measures adopted to mitigate the risks.

Moreover, the interplay between different data controllers regarding risk assessment may be the consequence of an existing relationship between manufacturers or software developers and users. In this sense, when a product or service makes specific use of personal data (e.g. healthcare equipment), the service provider or the manufacturer may carry out a general impact assessment of the data processing operations which can be performed involving this product or service. This does not remove the controller's obligation to carry out another DPIA on the specific use of this product/service and its potential implementation.

Regarding the manner in which the data controller should carry out the DPIA, it is worth pointing out that this assessment cannot be the last stage of development of a

---

a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks").

[102] See Article 29 Data Protection Working Party (n 42) 9.

[103] According to Article 29 Data Protection Working Party (n 42) 9, this case includes data processing performed in a public area that people passing by cannot avoid, or data processing" that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan".

[104] See Article 35.1. See also recital n. 92.

[105] See also Article 30 GDPR.

[106] See Article 29 Data Protection Working Party (n 42) 6.

product/service which uses personal information, but it must be part of a co-design product/service development. This requires active interaction between the project team and the data management or legal team (i.e. Data Protection Officer, data processor, Chief Information Security Officer) from the earliest stages of product/service development[107] and, where necessary, the active engagement of the potential stakeholders.

Regarding stakeholders' engagement, Article 35.9 states that controllers should seek the views of data subjects or their representatives "where appropriate". According to the Article 29 Working Party,[108] those views could be sought in a variety of ways, depending on the context (e.g. an internal or external study related to the purpose and means of the processing operation, a formal question to the staff representatives or trade/labour unions or a survey sent to the data controller's future customers). Moreover, if the data controller decides that seeking the views of data subjects is not appropriate, it should document its justification. Where data subjects are involved in the process, the data controller should document its final decision if it differs from the views of the data subjects.

Article 35 also mentions the need to safeguard the commercial or public interests or the security of processing operations in the case of stakeholders' engagement. In this regard, the solutions already proposed by legal scholars[109] and the Council of Europe[110] with regard to the disclosure of the results of impact assessment may be adopted. In this sense, confidential information may be provided in a separate annex to the assessment report, as suggested by the Guidelines on Big Data adopted by the Council of Europe.[111] In the same light, the Article 29 Working Party states that the published DPIA does not need to contain the whole assessment, but just a summary of the main findings to preserve controller's trade secrets or commercially sensitive information, and to avoid security risks for the data controller as well.

Although the Article 29 Working Party recognises that the GDPR does not include a duty to publish the results of the DPIA, the Working Party highlights how a publicly available assessment fosters trust in the controller and demonstrates accountability and transparency, particularly "where members of the public are affected by the processing operation", as in the case of data processing carried out by public authorities.[112]

In terms of internal organisation and procedure, the first step of the assessment procedure is to map and analyse the data flows involved in the data processing, outline the nature of the data processed, the data subjects potentially affected by the processing and the allocation of the data processing tasks. Based on this map, it is

---

[107] See also Article 29 Data Protection Working Party (n 42) 15.
[108] See Article 29 Data Protection Working Party (n 42) 13.
[109] See Wright, D. (2011). A framework for the ethical impact assessment of information technology. *Ethics Inf. Technol.* 13(3), 222; Richards, N.M. and King, J.K. (2013) Three Paradoxes of Big Data' *Stan. L. Rev. Online* 66, 41, 43; Mantelero, A. (2014). The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. *Comp. L. & Sec. Rev.* 30(6), 643, 655.
[110] See Council of Europe (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (n 5), Section IV, para 3.3 ("the results of the assessment process described in Section IV.2 should be made publicly available, without prejudice to secrecy safeguarded by law").
[111] See Council of Europe (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (n 5), Section IV, para 3.3.
[112] See Article 29 Data Protection Working Party (n 42) 17.

possible to identify potential risk areas, including cross-border data flows or data communications to third parties, as well as to estimate the likelihood and severity of risks.

The second step, based on the previous one, is the co-design of data processing. This requires both legal expertise and the specific skills needed by the given processing operation. In this phase, the data processing roadmap for a given product/service is reconsidered from a data protection perspective and the by-design solutions are adopted in response to the outcomes of the risk assessment.

At this stage, technical solutions, such as data retention times, possible use of anonymisation or pseudonymisation, as well as technical safeguards (e.g. encryption), or physical and logical organisational measures (e.g. database partitioning, decentralised storage systems, etc.) can be adopted. Moreover, data controllers should also consider the impact of cloud solutions or outsourcing strategies on these technical and organisational measures.

At the same time, data controllers should also consider whether it is appropriate to engage the data subjects in the assessment and co-design process. Engagement of data subjects and stakeholders in general may be critical for companies, since it can expose them to customers feedback. However, it could represent an opportunity to gain competitive advantage in terms of a better perception of risks or a more privacy-oriented image of the company. This is not only important in terms of corporate communication, but also raises customer awareness.

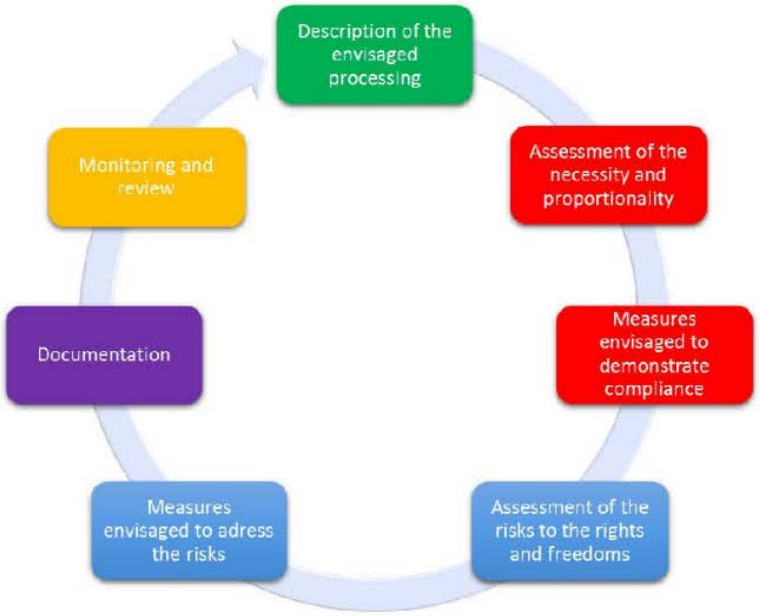
Lastly, data controllers should reflect on the integration of data processing risk management and the broader risk management duties and models of private companies and public entities. Such models are mainly focused on the organisational dimension and rarely pay attention to personal data. Given the increasing importance of information assets, risks associated with data use should be seen as a potential source of serious damages for enterprises and public bodies, in terms of both direct damage (loss of information, malfunctioning, etc.) and indirect damage (e.g. reputational damages).

For these reasons, a generic analysis of the potential impact on personal data (Article 32) in the early stages of each project should identify the major challenges and evaluate the need to adopt a broader risk assessment strategy, appointing people inside and outside the company to be engaged in the assessment procedure.[113] In this sense, risk management has a modular, scalable and circular structure, which may stop at the first phase (Article 32, no high risk), continue to the second one (DPIA, Article 35, high risk) or, in the most critical cases, reach the third (Article 36, prior consolation).

Since risk management is not a static evaluation, the assessment should be reviewed periodically or whenever circumstances arise which significantly affect the severity and likelihood of risks or introduce new ones. Following this review, the assessment may either become easier (e.g. if the risk is no longer high, the DPIA is no longer necessary) or more structured (increased risk severity/probability requires a formal DPIA or prior consultation with the Supervisory Authority).

---

[113] In terms of procedure, risk analysis should therefore be understood as a form of triage where priorities and interventions are determined based on the severity of the situation. If the situation is not serious, project managers and privacy teams should not need to complete too many forms and answer too.



Source: Article 29 Data Protection Working Party, *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*, 16.

3.3.3Prior consultation

Article 36 concerns those cases in which a formal risk analysis has been carried out by the controller, pursuant to Article 35, but the risk cannot be adequately mitigated. The data controller is therefore required to consult the competent supervisory authority (Article 36.1). This is not a completely new approach: Article 20 of Directive 95/46/EC gave Member States the power to submit certain types of processing to prior assessment and, if necessary, to define which cases were subject to such scrutiny.

Although the wording of Article 36.1 is not entirely clear when defining the cases in which prior consultation is required ("the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk"), the guidelines provided by the Article 29 Data Protection Working Party confirm that the key reference is to the notion of residual risk.[114] This means that the prior consultation is an ex-post evaluation, once the controller has identified the risk mitigation measures suggested by the DPIA: if a residual risk exists despite the adoption of these measures, prior consultation is required.

Recital 94 states that the lack of available solutions to mitigate this risk need not be absolute, in terms of no available technical or organisational measures. The recital talks about a lack of "reasonable" means. Potential measures are reasonable when

[114] See Article 29 Data Protection Working Party (n 42) 17.

they are available at an affordable implementation cost. This reference to a reasonable cost of implementation – also made with regard to the general assessment in Article 32 and to privacy by-design solutions – is critical in terms of an effective application of the principle of proportionality in the context of data processing risk management.

Following the data controller's request for consultation, the Supervisory Authority must firstly evaluate whether the risk assessment has been correctly conducted by the controller. If the controller has failed to identify or mitigate the risk sufficiently, the Supervisory Authority should provide written advice to the controller and, where applicable, to the processor, within eight weeks of receiving the request.[115]

To facilitate the evaluation carried out by the Supervisory Authority, the controller must submit the outcome of the data protection impact assessment and a description of the measures envisaged to mitigate the risk (Article 36.3.c and e).[116] Where applicable, the controller should also inform the supervisory authority of the various responsibilities of the controller and processor, and those of the joint controllers, if any.[117]

If, on the basis of this information, the Supervisory Authority judges that the data controller has correctly conducted the risk assessment and taken reasonable measures to tackle the risk, but a residual risk remains, the authority must stop data processing. It is not clear here whether the Supervisory Authority may authorise, on an exceptional basis, data processing operations which present a residual high risk, but may be justified in light of a broader balancing of interests.[118]

Finally, national laws may add specific cases in which data controllers are required to consult with, and obtain prior authorisation from, Supervisory Authorities. These cases may only concern data processing performed by a controller for the performance of a task carried out in the public interest.

4. The limits of the DPIA

The GDPR has undoubtedly increased the level of accountability of data controllers and the DPIA represent an important element of this change. Nevertheless, the solution adopted suffers two limits: the existing relationship between risk assessment and purposes of data processing and the focus of the risk assessment on the individual dimension.

---

[115] This period may be extended by six weeks, depending on the complexity of the data processing. In this case, the supervisory authority must inform the controller and, where applicable, the processor, of any such extension within one month of receiving the request for consultation together with the reasons for the delay. The period may also be suspended until the supervisory authority has obtained the information needs for the purposes of the consultation (Article 36.2).

[116] See also Recital 94.

[117] The controller should also provide the key information about the data processing (i.e. the purposes and means of the intended processing, the contact details of the data protection officer) and any other information requested by the supervisory authority (Article 36.3).

[118] Article 29 Data Protection Working Party (n 42) 19 does not provide any specific indication on this point.

Although, from a systemic perspective, the first of these limits is less important than the latter, the existing relationship between risk assessment and purposes of data processing[119] propose again the criticisms concerning the application of the purpose limitation principle.

Indeed, any assessment is related to the use of data for a specific purpose and, according to Regulation (EU) 2016/679, data processing purposes should be "specific, explicit and legitimate", and defined at the moment of data collection.[120] Nevertheless, this is not consistent with the transformative use of data by private and public bodies through big data analytics.

The second, most relevant, limit concerns the nature of the risk-assessment required by the Regulation. In this regard, the notion of risk adopted in the new Regulation focuses on material or non-material damages that prejudice the "rights and freedoms of natural persons".[121] This is in line with a rights-based approach in risk management, which focuses on rights protection and not on a general trade-off between risks and benefits.[122]

According to this approach, when a risk of prejudice exists and cannot be mitigated or excluded, data processing becomes unlawful, despite the presence of any legitimate grounds, such as the data subject's consent. In light of this, Recital no. 75 of the Regulation provides a long list of cases where data processing is considered unlawful.

It should be pointed out that this recital does not limit these cases to the security of data processing, but also takes into account the risk of discrimination and "any other significant economic or social disadvantage". This notion of risk impact, which is echoed in Article 35 of the Regulation, represents an important step in the direction of an impact assessment of data processing that is no longer primarily focused on data security[123] but evolves into a more robust and broader assessment of the different implications of data use.[124]

---

[119] See Article 35 (1) of Regulation (EU) 2016/679 ("Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons") and 35(7)(b) ("[The assessment shall contain at least] an assessment of the necessity and proportionality of the processing operations in relation to the purposes").

[120] See Article 5(1)(b) of Regulation (EU) 2016/679.

[121] See Recital no. 75 of Regulation (EU) 2016/679.

[122] According to the risk/benefit approach, the assessment should be based on the comparison between the importance of benefits and the sum of all risks, without any distinction regarding the nature of risks and benefits. For instance, economic benefits may prevail over individual rights. On the other hand, the risk mitigation approach assumes that some interests (e.g. fundamental rights) are prevailing and cannot be compared with other interests that have a lower relevance. As a consequence, the risk mitigation approach focuses on the potential prejudice to fundamental rights and suggests adequate measures to reduce this risk or, where feasible, to exclude it. On the different classifications of risks related to privacy and data protection, see also Wright & Raab (n 4).

[123]See Article 32 of Regulation (EU) 2016/679.

[124] See also Article 29 Data Protection Working Party (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, 4 April 2017, revised 4 October 2017 (n 42) 15. ("the reference to "the rights and freedoms" of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion"); Article 29 Data protection Working Party (2014). Statement on the role of a risk-based approach in data protection legal frameworks (n 70).

Attention to the economic and social implications of data use assumes significant relevance in the big data context, where analytics become part of decision-making processes and may have negative impacts on individuals, in terms of discrimination[125] rather than in terms of data security.[126] However, the provisions of the Regulation do not offer an adequate framework for the assessment of this kind of negative outcome.

The risk-mitigation approach adopted by the Regulation still seems far from the idea of an assessment which adequately considers also the ethical and social impacts of data use.[127] This broad assessment should be a multiple and participative risk-assessment process where the potential negative outcomes of data processing are not only measured in terms of information protection, but also encompass the societal consequences of data uses and their impact on the application of ethical values.

The lack of this wider perspective represents a limit, since the use of big data analytics in decision-making processes raises important questions regarding the values that should drive the future algorithmic society. Moreover, focusing on the collective dimension, rule-makers should also reflect on the role that the different social stakeholders can play in assessing the societal impacts of data use.[128] For this reason, one of the main goals of the Virt-EU is to outline a Privacy, Ethical and Social Impact Assessment which goes beyond these limits.

4.1.1 DPIA and PESIA: from an individual to a collective dimension in data protection

Innovative technologies and powerful analytics make it possible to collect and analyse huge amounts of data to try and identify patterns in the behaviour of groups

---

[125] See The White House, Executive Office of the President (2016). Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf> accessed 4 March 2017. See also European Data Protection Supervisor (2015). Opinion 7/2015. Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf> accessed 12 February 2017.

[126] See also European Parliament (2017). European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//EN&language=EN> accessed 16 March 2017.

[127] With regard to the ethical assessment in research and innovation, see Shelley-Egan, C. et al. (2014). SATORI Deliverable D2.1 Report (handbook) of participatory processes, 42-44 <http://satoriproject.eu/work_packages/dialogue-and-participation/> accessed 15 February 2017 ("Ethical impact assessment of research and innovation typically considers potential societal harms, risks and implications for fundamental rights, justice, well-being of citizens and the common good. Such assessments may require a consideration of potential impacts on health, the environment, work, leisure, social relations, politics, values, and so on. To achieve this, ethical impact assessment often combines ethical analysis with social impact analysis, futures studies, scenario analysis, and technology assessment. Engagement with stakeholders and public dialogue are other actions within ethical impact assessment, as stakeholders can help to anticipate utilisations and impacts, and can voice their concerns and interests as part of the process of ethics assessment").

[128] See below Section 4.1.3. See also 3. Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection. *Computer Law and Security Review*, 32 (2): 249-251.

of individuals[129] and to take decisions that affect the internal dynamics of groups with consequences for the collective issues of the people involved.

Nevertheless, these groups are different from those considered in the literature on group privacy, since they are created by data gatherers selecting specific clusters of information. Data gatherers shape the population they set out to investigate. They collect information about various people who do not know the other members of the group and, in many cases, are not aware of the consequences of their belonging to a group.[130] This is the case of consumer group profiling,[131] scoring solutions[132] and predictive policing applications.[133]

The issues relating to data protection that arise from this new situation are different from the issues of individual data protection and group privacy. We are neither in the presence of forms of analysis that involve only individuals, nor in the presence of groups in the traditional sociological meaning of the term, given group members' lack of awareness of themselves as part of a group and the lack of interactions among people grouped into various clusters by data gatherers.

We must therefore extend the field of investigation to the collective interests of the persons whose personal data is being collected, analysed and grouped. The differing nature of these groups of individuals requires a different approach that cannot be exclusively based on individual rights.

The new scale entails the recognition of a new layer, represented by the rights of groups of individuals to the protection of their collective privacy and data protection. Moreover, since the predictive nature of big data analytics is designed to assist

---

[129] Moreover, this is also possible without directly identifying data subjects; see Zwitter, A. (2014). Big Data ethics. *Big Data & Society* 1, 4-5. See also Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA L. Rev.* 57, 1701-1777; Golle, P. (2006). Revisiting the uniqueness of simple demographics in the US population. In Juels, A. (ed). *Proc. 5th ACM workshop on Privacy in electronic society* (ACM 2006) 77-80; Sweeney, L. (2000). Simple Demographics Often Identify People Uniquely (Carnegie Mellon University) <http://dataprivacylab.org/projects/identifiability/paper1.pdf> accessed 24 January 2015; Sweeney, L. (2000). Foundations of Privacy Protection from a Computer Science Perspective. In *Proc. Joint Statistical Meeting, AAAS, Indianapolis* <http://dataprivacylab.org/projects/disclosurecontrol/paper1.pdf> accessed 24 January 2015.

[130] See Hildebrandt, M. (2010). Defining Profiling: A New Type of Knowledge?. In Hildebrandt, M. & Gutwirth, S. (eds.), Profiling the European Citizen. Cross-Disciplinary Perspective (Netherlands : Springer 2010) 19-20. See also Executive Office of the President of the United States-Council of Economic Advisers (2015). *Big Data Differential Pricing*, 18 <https://www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf> accessed 25 March 2015; Hildebrandt, M. (2006) Profiling: From Data to Knowledge. The challenges of a crucial technology. *Datenschutz und Datensicherheit* 30(9), 549-550.

[131] See also Calo, R. (2014). Digital Market Manipulation. *George Washington Law Review* 82, 995.

[132] See Federal Trade Commission (2014). Data Brokers: A Call for Transparency and Accountability <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparencyaccountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> accessed 27 February 2014. But see Articles 18 and 20 of the Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010.

[133] Cfr. Perry, W.L., McInnis, B., Price, C.C., Smith, S.C., & Hollywood, J.S. (2013). Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations (The RAND Corporation).

decisions that affect a plurality of individuals in various fields, we must also consider the social and ethical effects associated with this type of analysis.[134]

This kind of approach differs from the theoretical framework proposed by legal scholars in shaping the notion of group privacy, but it can give a specific answer to the issues arising from the present and future scenarios of the data-driven society.

4.1.2 Collective data protection and its rationale

The collective dimension of data protection has its roots in the individual's right to privacy and shares some similarities with group privacy, but it differs from both these previous notions. On the one hand, notions of individual privacy and data protection do influence the definition of the boundaries of this collective dimension, but the greater scale affects the morphology of the interests involved and their enforcement. At the same time, group privacy – as hitherto described by legal scholars – represents the notion that is closest to the idea of collective data protection.

On the other hand, collective data protection does not necessarily concern facts or information referring to a specific person,[135] as with individual privacy and data protection. Nor does it concern clusters of individuals who can be considered groups in the sociological sense of the term. In addition, collective rights are not necessarily a large-scale representation of individual rights and related issues. Finally, collective data protection concerns non-aggregative collective interests,[136] which are not the mere sum of many individual interests.

The importance of this collective dimension depends on the fact that the approach to classification by modern algorithms does not merely focus on individuals, but on groups or clusters of people with common characteristics (e.g. customer habits, lifestyle, online and offline behaviour, etc.).[137] Data gatherers are mainly interested in studying groups' behaviour and predicting this behaviour, rather than in profiling single users. Data-driven decisions concern clusters of individuals and only indirectly

---

[134] See Article 29 Data Protection Working Party (2014). Statement on the role of a risk-based approach in data protection legal frameworks (n 70), 4; Schwartz, P.M. (2011). Data Protection Law and the Ethical Use of Analytics, 22-26. <http://www.huntonfiles.com/files/webupload/CIPL_Ethical_Undperinnings_of_Analytics_Paper.pdf> accessed 27 February 2014; Wright (n 109) 199–226. See also Floridi, L. (2014). *The 4TH Revolution. How the Infosphere is Reshaping Human Reality* (Oxford : Oxford University Press) 189-190; Nissenbaum, H. (2010). *Privacy in Context. Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press) 231; Calo, R.M. (2013). Consumer Subject Review Boards: A Thought Experiment. *Stan. L. Rev. Online* 66, 97, 101-102; Dwork, C. & Mulligan, D.K. (2013). It's not Privacy and It's not Fair. *Stan. L. Rev. Online* 66, 35, 38; Bygrave (n 52) 61-62, 339; Cohen (n 68); Crawford, K. et al. (2013). Big Data, Communities and Ethical Resilience: A Framework for Action, 4 <http://www.rockefellerfoundation.org/app/uploads/71b4c457-cdb7-47ec-81a9-a617c956e6af.pdf> accessed 5 April 2015.

[135] In many cases, private companies and governments have no interests in profiling single customers or citizens, but wish to discover the attitudes of clusters of individuals. Their main purpose is to predict future behaviours of segments of the population to achieve economic or political goals. See Bollier (n 67).

[136] See Newman, D.G. (2004). Collective Interests and Collective Rights. *American Journal of Jurisprudence* 49(1), 127, 131. See also below in the present section. On the contrary, an aggregative approach seems to be consistent with the notion of group privacy described by Bloustein, E.J. (1978). *Individual and Group Privacy* (New Brunswick, N.J.: Transaction Books) 123-186.

[137] See also below in the text.

affect the members of these clusters. One example of this is price discrimination based on age, habits or wealth.

The most important concern in this context is the protection of groups from potential harm due to invasive and discriminatory data processing. The collective dimension of data processing is mainly focused on the use of information,[138] rather than on secrecy[139] and data quality.

We need to adopt a broader notion of discrimination here, one that encompasses two different meanings. In a negative sense, discrimination is "the unjust or prejudicial treatment of different categories of people". In a more neutral and potentially positive sense, though, discrimination may be the "recognition and understanding of the difference between one thing and another".[140] Both these dimensions assume relevance in the context of big data analytics.

We will focus below on the first meaning, since the unfair practices characterised by discriminatory purposes are generally forbidden and sanctioned by law.[141] This section concerns involuntary forms of discrimination in cases where big data analytics provide biased representations of society.[142]

For example, in 2013 a study examined the advertising provided by Google AdSense and found statistically significant racial discrimination in advertisement delivery.[143] Similarly, Kate Crawford has pointed out certain "algorithmic illusions"[144] and described the case of the City of Boston and its StreetBump smartphone app to passively detect potholes. The application had a signal problem, due to the bias generated by the low penetration of smartphones among lower income and older residents. While the Boston administration took this bias into account and solved the

---

[138] See Cate F.H. & Mayer-Schönberger, V. (2013). *Data Use and Impact. Global Workshop* (The Center for Information Policy Research and The Center for Applied Cybersecurity Research, Indiana University 2013) iii <http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf> accessed 27 February 2014.

[139] See Bloustein (n 136) 182.

[140] See <http://www.oxforddictionaries.com/it/definizione/inglese/discrimination> accessed 29 January 2015.

[141] See *inter alia* European Commission (2013). Developing Anti-Discrimination Law in Europe. The 28 EU Member States, the Former Yugoslav Republic of Macedonia, Iceland, Liechtenstein, Norway and Turkey compared <http://www.non-discrimination.net/content/media/Developing%20Anti-Discrimination%20Law%20in%20Europe%20EN%2029042014%20WEB.pdf> accessed 28 March 2015; Ellis, E. & Watson, P. (2015). *EU Anti-Discrimination Law* (Oxford : Oxford University Press). See also Article 14 of the Convention for the Protection of Human Rights and Fundamental Freedoms; Article 21 of the Charter of Fundamental Rights of the European Union; Article 19 of the Treaty on the Functioning of the European Union; Directive 2000/43/EC; Directive 2000/78/EC. See also Schreurs, W., Hildebrandt, M., Kindt, E. & Vanfleteren,M. (2010). Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. In Hildebrandt, M. & Gutwirth, S. (eds.). Profiling the European Citizen. Cross-Disciplinary Perspective. (Dordrecht: Springer) 258-264.

[142] See Citron, D.K. & Pasquale, F. (2014). The Scored Society: Due Process For Automated Predictions. *Wash. L. Rev.* 89, 14; Burnbaum, B. (2013). *Insurers' Use of Credit Scoring for Homeowners in Ohio: A Report to the Ohio Civil Rights Commission*.

[143] See Sweeney, L. (2013). Discrimination in Online Ad Delivery. Communications of the ACM 56(5), 44-54.

[144] Crawford, K. (2013). Algorithmic Illusions: Hidden Biases of Big Data. Presentation at Strata 2013, <https://www.youtube.com/watch?v=irP5RCdpilc> accessed 15 March 2015.

problem, less enlightened public officials might underestimate such considerations and make potentially discriminatory decisions.[145]

Another example is the Progressive case, in which an insurance company obliged drivers to install a small monitoring device in their cars in order to receive the company's best rates**.** The system considered as a negative factor driving late at night, but did not take into account the potential bias against low-income individuals, who are more likely to work night shifts, compared with late-night party-goers, "forcing them [low-income individuals] to carry more of the cost of intoxicated and other irresponsible driving that happens disproportionately at night".[146]

These cases represent situations in which a biased representation of groups and society results from flawed data processing[147] or a lack of accuracy in the representation.[148] This produces potentially discriminatory effects as a consequence of the decisions taken on the basis of analytics.

On the other hand, the other sense of discrimination involving different treatment of different situations may represent an intentional goal for policy makers, which is in line with the rule of law. This is the case of law and enforcement bodies and intelligence agencies, which adopt solutions to discriminate between different individuals and identify targeted persons. Here there is a deliberate intention to treat given individuals differently, but this is not unfair or illegal providing it is within existing legal provisions. Nonetheless, as in the previous case, potential flaws or a lack of accuracy may cause harm to citizens.

For instance, criticisms have been raised with regard to the aforementioned predictive software adopted in recent years by various police departments in the US. Leaving aside the constitutional profiles associated with these applications and the peculiar balance of interests of this use of data, there have been cases where people were named as potential offenders due to merely remote connections with authors of serious crimes.[149] Criticisms also concern the use of risk assessment procedures based on analytics coupled with a categorical approach (based on typology of crimes and offenders) in U.S. criminal sentencing.[150]

---

[145]See Crawford, K. (2013). The Hidden Biases in Big Data. *Harv. Bus. Rev*., April 1, 2013, <https://hbr.org/2013/04/the-hidden-biases-in-big-data> accessed 29 January 2015. Similar considerations can be made in the case of the predictive policing systems mentioned above in the text and fn. 133. See also Lerman, J. (2013). Big Data and Its Exclusions. *Stan. L. Rev. Online* 66, 55.

[146] See Rieke, A., Robinson, D. & Yu, H. (2014). Civil Rights, Big Data, and Our Algorithmic Future. A September 2014 report on social justice and technology, 6 <http://bigdata.fairness.io/wpcontent/uploads/2014/09/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_2014-09-12.pdf> accessed March 10, 2015.

[147] This is the case of the errors that affect the E-Verify system, which is used in the US to verify if a new worker is legally eligible to work in the US. See Rieke, Robinson & Yu (n 146) 12-14; National Immigration Law Center (2013). *Verification Nation*, 6 <www.nilc.org/document.html?id=957> accessed 29 January 2015.

[148] See also Oscar H. Gandy Jr., 'Exploring Identity and Identification in Cyberspace' (2000) 14 Notre Dame J.L. Ethics & Pub. Pol'y 1085, 1100 <http://scholarship.law.nd.edu/ndjlepp/vol14/iss2/10> accessed 10 July 2015, 1099-1100.

[149] See Gorner, J. (2013). Chicago police use 'heat list' as strategy to prevent violence. Officials generate analysis to predict who will likely be involved in crime, as perpetrator or victim, and go door to door to issue warnings. *Chicago Tribune* (Chicago, 21 August 2013) <http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list> accessed 25 February 2015.

[150] See U.S. Department of Justice - Criminal Division, Office of the Assistant Attorney General (2014). Annual letter, 6-7, 13 <http://www.justice.gov/criminal/foia/docs/2014annual-letter-final-

Discrimination – the different treatment of different situations – also appears in commercial contexts to offer tailored services to consumers. In this case, where the interests are of a purely private nature, commercial practices may lead to price discrimination[151] or the adoption of differential terms and conditions depending on the assignment of consumers to a specific cluster.[152]

Thus, consumers classified as "financially challenged" belong to a cluster "[i]n the prime working years of their lives […] including many single parents, struggl[ing] with some of the lowest incomes and little accumulation of wealth". This implies the following predictive viewpoint, based on big data analytics and regarding all consumers in the cluster: "[n]ot particularly loyal to any one financial institution, [and] they feel uncomfortable borrowing money and believe they are better off having what they want today as they never know what tomorrow will bring".[153] It is not hard to imagine the potential discriminatory consequences of similar classifications with regard to individuals and groups.

It should be noted that these forms of discrimination are not necessarily against the law, especially when they are not based on individual profiles and only indirectly affect individuals as part of a category, without their direct identification.[154] For this

---

072814.pdf> accessed 29 January 2015 ("This phenomenon ultimately raises constitutional questions because of the use of groupbased characteristics and suspect classifications in the analytics. Criminal accountability should be primarily about prior bad acts proven by the government before a court of law and not some future bad behavior predicted to occur by a risk assessment instrument. Second, experience and analysis of current risk assessment tools demonstrate that utilizing such tools for determining prison sentences to be served will have a disparate and adverse impact on offenders from poor communities already struggling with many social ills"). See also Administrative Office of the United States Courts - Office of Probation and Pretrial Services (2011). An Overview of the Federal Post Conviction Risk Assessment <http://www.uscourts.gov/uscourts/FederalCourts/PPS/PCRA_Sep_2011.pdf> accessed 29 January 2015; Underwood, B.D. (1979). Law and the Crystal Ball: Predicting Behavior with Statistical Inference and Individualized Judgment. *Yale Law J.* 88, 1408-1413.

[151] Price discrimination or "differential pricing" is the practice of charging customers different prices for the same product, see Executive Office of the President of the United States-Council of Economic Advisers (n 130), 4-5. The cases considered in this article mainly concern the so-called third-degree price differentiation, which occurs when sellers charge different prices to different segments of the market. See also Rosenblat, A. et al. (2014). Data & Civil Rights: Consumer Finance Primer <http://www.datacivilrights.org/pubs/2014-1030/Finance.pdf> accessed 15 March 2015.

[152] See Executive Office of the President of the United States-Council of Economic Advisers (n 130); Federal Trade Commission (n 132) 3, 19-21; Dixon, P. & Gellman, R. (2014). The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future <http://www.worldprivacyforum.org/wpcontent/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf> accessed 10 March 2015. See also Lambert, T.C. (1999). Fair Marketing: Challenging Pre-Application Lending Practices. *Geo. L. J.* 87, 2182.

[153] See Federal Trade Commission (n 132) 20, fn. 52.

[154] See also Article 4 (4) GDPR; Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (n 31); Article 29 Data Protection Working Party (2013). Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf> accessed 29 March 2015; Article 29 Data Protection Working Party (2012). Opinion 01/2012 on the data protection reform proposals' (2012) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf> accessed 29 March 2015. Regarding the decisions that affect an individual as member of a specific cluster of people, it should be noted that in many cases these decisions are not based solely on automated processing; see Zarsky, T.Z. (2013). Transparent Predictions. *U. Ill. L. Rev.* 4, 1503, 1518-1519. In this sense, credit scoring systems have reduced but not removed human intervention on credit evaluation. At the same time, classifications often regard

reason, existing legal provisions against individual discrimination might not be effective in preventing the negative outcomes of these practices, if adopted on a collective basis. Still, such cases clearly show the importance of the collective dimension of the use of information about groups of individuals.

Within the EU, such data analysis focusing on clustered individuals may not represent a form of personal data processing,[155] since the categorical analytics methodology does not necessarily make it possible to identify a person.[156] Moreover, group profiles can be made using anonymised data.[157] This reduces the chances of individuals taking action against biased representations of themselves within a group or having access to the data processing mechanisms, since the anonymized information used for group profiling cannot be linked to them.[158] Even so, group profiling does make it possible to take decisions affecting a multiplicity of individuals.[159] In this sense, the main target of the collective dimension of data processing is not the data subject, but the clusters of people created by big data gatherers.

identified or identifiable individuals. See Article 29 Data Protection Working Party (2010). Opinion 2/2010 on online behavioural advertising <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf accessed 29 March 2015>accessed 29 March 2015; Data Protection Working Party (2013). Working Document 02/2013 providing guidance on obtaining consent for cookies, 5-6 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf> accessed 29 March 2015. Regarding the applicability of the Data Protection Directive in case of automated profiling, see Bygrave, L.A. (2001). Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling. *Comp. Law & Sec. Rev.* 17 (1), 17-24; Schreurs, Hildebrandt, Kindt & Vanfleteren (n 141) 241-257.

[155] See Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> accessed 25 January 2015.

[156] On the blurring of the border between group profiles and personalized profiles, see also Hildebrandt (n 130).

[157] On the limits of anonymization in the big data context, see Narayanan, Huey & Felten (n 7); Arvind Narayanan, Edward W. Felten, 'No silver bullet: De-identification still doesn't work' (2014) <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf> accessed 25 March 2015; Ohm (n 129); United States General Accounting Office (2011). Record Linkage and Privacy. Issues in creating New Federal Research and Statistical Information 68-72 <http://www.gao.gov/assets/210/201699.pdf> accessed 14 December 2013; Sweeney, L. (2015). Only You, Your Doctor, and Many Others May Know. *Technology Science* 2015092903. September 29, 2015 <http://techscience.org/a/2015092903> accessed 28 November 2015; Sweeney, L. (2000) Simple Demographics Often Identify People Uniquely (n 129); Sweeney, 'Foundations of Privacy Protection from a Computer Science Perspective' (n 129).

[158] See Bygrave (n 52) 319; Schreurs, Hildebrandt, Kindt & Vanfleteren (n 141) 252-253; Koops, B-J. (2014). The trouble with European data protection law. Int'l. Data Privacy Law 4(4), 257-258.

[159] This happens, for instance, in the management of smart cities or in the decisions adopted on the basis of credit scoring systems. Against this background, Mireille Hildebrandt observed that "once a profile is linked to an identifiable person – for instance in the case of credit scoring – it may turn into a personal data, thus reviving the applicability of data protection legislation", see Hildebrandt (n 130) 550. See also Vedder, A.H. 1997. Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations. In Moore, G. (ed), *Business Ethics: Principles and Practice* (Sunderland : Business Education Publishers) ("Categorial privacy can be considered as relating to information (1) which was originally taken from the personal sphere of individuals, but which, after aggregation and processing according to statistical methods, is no longer accompanied by identifiers indicating individual natural persons, but, instead, by identifiers of groups of persons, and (2) which, when attached to identifiers of groups and when disclosed, is apt to cause the same kind of negative consequences to the members of those groups as it would for an individual person if the information were accompanied by identifiers of that individual").

The interests that assume relevance therefore have a supra-individual nature and a collective dimension,[160] which are not adequately addressed by the existing data protection legal framework. These interests may be shared by an entire group without conflicts between the views of its members (aggregative interests) or with conflicts between the opinions of its members (non-aggregative interests).[161] If the group is characterised by non-aggregative interests, the collective nature of the interest is represented by the fundamental values of a given society (e.g. environmental protection).

The notion of collective non-aggregative interests seems to be the best way to describe the collective dimension of data protection, which becomes important in the discrimination cases mentioned above. Although individuals may have different opinions about the balance between the conflicting interests,[162] there are some collective priorities concerning privacy and data-protection that are relevant to the general interest. Here the rationale for collective data protection is mainly focused on the potential harm to groups caused by extensive and invasive data processing.

4.1.3 Collective interests in data protection and their representation

Data protection is a context-dependent notion, which varies from culture to culture and across historical periods.[163] In the same way, its collective dimension is necessarily influenced by historical and geographical variables and is the result of actions by policymakers. For these reasons, it is impossible to define a common and fixed balance between collective data protection and conflicting interests.

There are jurisdictions that give greater priority to national and security interests, which in many cases prevail over individual and collective data protection; whereas, in some countries extensive forms of social surveillance are considered disproportionate and invasive. Therefore, any balancing test must focus on a specific social context in a given historical moment.[164] As it has been pointed out in the literature,[165] defining prescriptive ethical guidelines concerning the values that should govern the use of big data analytics and the related balance of interests is problematic.

Given such variability, from a theoretical perspective a common framework for a balancing test can be found in the values recognised by international charters of

---

[160] See Newman (n 136) 131.
[161] See Newman (n 136) 131-132 makes this distinction and defines these two categories of interests respectively as “shared” and “collective” interests. As observed by Finnis, a collective interest in which the conflict is diminished may become a shared interest. See Finnis, J. (1984). The Authority of Law in the Predicament of Contemporary Social Theory. *J.L. Ethics & Pub. Pol'y* 1, 115, 135-136.
[162] In this sense, an extensive group profiling for commercial purposes can be passively accepted, considered with favour or perceived as invasive and potentially discriminatory. The same divergence of opinions and interests exists with regard to government social surveillance for crime prevention and national security, where part of the population is in favour of surveillance, due to concerns about crime and terrorism.
[163] See Westin (n 56) 183-187; Whitman, J.Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale L.J.* 113, 1151-1221; Bygrave (n 52); Nissenbaum (n 134); Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific?. *Journal of Social Issues* 33(3) 66–84.
[164] See in this sense the different attitudes of U.S. government with regard to surveillance, before and after the September 11, 2001 terrorist attacks. See also Bygrave, L.A. (2004). Privacy Protection in a Global Context. A Comparative Overview. *Scandinavian Studies in Law* 7, 319, 329.
[165] See Wright (n 109), 200.

fundamental rights. These charters provide a baseline from which to identify the values that can serve to provide ethical guidance and define the existing relationships between these values.[166]

In addition, the context-dependent framework of values and the relationship between conflicting interests and rights needs to be specified with regard to the actual use of big data analytics. In Europe, for instance, commercial interests related to credit score systems can generally be considered compatible with the processing of personal information, providing that the data is adequate, relevant and not excessive in relation to the purposes for which it is collected.[167] Even so, specific big data analytics solutions adopted by some companies for credit scoring purposes may lead to a disproportionate scrutiny of a consumer's private life. The same reasoning can also be applied to smart mobility solutions, which can potentially lead to extensive social surveillance. This means a prior case-by-case risk-assessment is necessary to mitigate the potential impact of these solutions on data protection and individual freedoms.

This "in-context" balance of conflicting interests is based on an impact assessment that, in the presence of complex data collection and processing systems,[168] should not be conducted by consumers or companies, but must entail an active involvement of various stakeholders. Against this background, an important aspect of the protection of collective interests relating to personal information is an analysis of the existing conflicting interests.

Here it is useful to briefly consider the fields in which the group dimension of data protection is already known in more traditional contexts which are not characterised by extensive data collection and use of analytics. For instance, labour law recognises this collective dimension of rights and the dualism between individuals and groups.[169] Under certain circumstances, trade unions and employees' representatives may concur in taking decisions that affect the employees and have an impact on data protection in the workplace.[170]

Collective agreement on these decisions is based on the recognition that the power imbalance in the workplace means that, in some cases, the employee is unaware of the implications of employer's policies (e.g. employers' workplace surveillance practices). Moreover, in many cases, this imbalance makes it difficult for employees to object to the illegitimate processing of their data.

Entities representing collective interests (e.g. trade unions) are less vulnerable to power imbalance and have a broader vision of the impact of the employer's policies

---

[166] See Wright (n 109) 201-202.
[167] See Articles 18 and 20 of the Directive 2014/17/EU. See also Article 8 of the Directive 2008/48/EC on credit agreements for consumers and repealing Council Directive 87/102/EEC.
[168] Moreover, these systems are influenced by lock-in effects. There are two different kinds of lock-ins: technological lock-in and social lock-in. The first is related to the technological standards and data formats that are adopted by service providers. This lock-in represents a limit to data portability and migration from one service to another. The second lock-in (social lock-in) is related to the dominant position held by some big players. This lock-in is evident, for example, in the social networks market, where there is an incentive to remain on a network, given the numbers of social relationships created by users.
[169] See e.g. Italian Articles 4 and 8, Act 300, 20 May 1970 (Statute of the Workers' Rights).
[170] See also Bygrave, L.A. & Schartum, D.W. (2009). Consent, Proportionality and Collective Power. In Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C. & Nouwt, S. (eds.). *Reinventing Data Protection?* (Dordrecht : Springer) 170.

and decisions. It should also be noted that the employer's unfair policies and forms of control are often oriented towards discriminatory measures that affect individual workers, even though they are targeted at the whole group.

This collective representation of common interests is also adopted in other fields, such as consumer protection and environmental protection. These contexts are all characterised by a power imbalance affecting one of the parties directly involved (employees, consumers or citizens). Furthermore, in many cases the conflicting interests refer to contexts where the use of new technologies makes it hard for users to be aware of the potential negative implications.

The same situation of imbalance often exists in the big data context, where data subjects are not in a position to object to the discriminatory use of personal information by data gatherers.[171] Data subjects often do not know the basic steps of data processing,[172] and the complexity of the process means that they are unable to negotiate their information and are not aware of the potential collective prejudices that underlay its use.[173] This is why it is important to recognise the role of entities representing collective interests, as happens in the above cases.

Employees are part of a specific group, defined by their relationship with a single employer; therefore, they are aware of their common identity and have mutual relationships. By contrast, in the big data context, the common attributes of the group often only become evident in the hands of the data gatherer.[174]

Data subjects are not aware of the identity of the other members of the group, have no relationship with them and have a limited perception of their collective issues. Furthermore, these groups shaped by analytics have a variable geometry and individuals can shift from one group to another.

This does not undermine the idea of a representing collective data protection interests. On the contrary, this atomistic dimension makes the need for collective representation more urgent. However, it is hard to imagine representatives appointed by the members of these groups, as is instead the case in the workplace.

---

[171] In the digital economy, consumers often accept not having an effective negotiation of their personal information, due to market concentration and related social and technological lock-ins.
[172] See also Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science* 347(6221), 509-514.
[173] The complexity of data processing in the big data environment does not offer users a real chance to understand it and make their choice. See Pasquale, F. (2015). *The Black Box Society. The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press) 143-144; Brandimarte, L., Acquisti, A. & Loewenstein, G. (2010). Misplaced Confidences: Privacy and the Control Paradox. Ninth Annual Workshop on the Economics of Information Security <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-SPPS.pdf> accessed 27 February 2014; Turow, J., Hoofnagle, C.J., Mulligan, D.K. & Good, N. (2007). The Federal Trade Commission and Consumer Privacy in the Coming Decade. *ISJLP* 3, 723-749 <http://scholarship.law.berkeley.edu/facpubs/935> accessed 27 February 2014; Federal Trade Commission (n 132) 42. On the limits of the traditional notices, see also Calo, R.M. (2013). Against Notice Skepticism in Privacy (and Elsewhere). *Notre Dame L. Rev.* 87(3), 1027, 1050-1055 <http://scholarship.law.nd.edu/ndlr/vol87/iss3/3> accessed 27 February 2014; Solove, D.J. (2013). Introduction: Privacy Self-management and The Consent Dilemma. *Harv. L. Rev.* 126, 1880, 1883-1888; World Economic Forum (2013). *Unlocking the Value of Personal Data: From Collection to Usage*, 18 <http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf> accessed 27 February 2014.
[174] See also Bygrave (n 52) 283-284.

In this sense there are similarities with consumer law, where there are collective interests (e.g. product security, fair commercial practices), but the potential victims of harm have no relationship to one another. Thus, individual legal remedies must be combined with collective remedies.[175] Examples of possible complementary solutions are provided by consumer law, where independent authorities responsible for consumer protection, class action lawsuits and consumer associations play an important role.

In the field of big data analytics, the partially hidden nature of the processes and their complexity probably make timely class actions more difficult than in other fields. For instance, in the case of a product liability, the damages are often more evident, making it easier for the injured people to react.[176] On the other hand, associations that protect collective interests can play an active role in facilitating reaction to unfair practices and, moreover, they can be involved in a multi-stakeholder risk assessment of the specific use of big data analytics.[177]

The involvement of such bodies requires specific procedural criteria to define the entities which may act in the collective interest.[178] This is more difficult in the context of big data, where the groups created by data gatherers do not have a stable character. In this case, an assessment of the social and ethical impact of analytics may provide the opportunity to discover how data processing affects collective interests and thus identify the potential stakeholders.[179]

4.2 A first outline of the main elements of the PESIA model

The adoption of a multiple participatory impact assessment, which encompasses ethical and social values, may represent the conclusion of the process that has characterized the evolution of accountability in data processing over the years. Nevertheless, the adoption of a mandatory Privacy, Ethical and Social Impact Assessment is still far to be feasible.

The GDPR is the result of a long negotiation between different stakeholders. In this sense, the DPIA (with its limits) represents a compromise between the need to adopt a higher level of accountability and the intent to maintain the existing business models developed by the main players of digital economy.

---

[175] The same approach has been adopted in the realm of anti-discrimination laws; see European Commission (n 141). See also Farkas, L. (2014). Collective actions under European anti-discrimination law. *European Anti-Discrimination L. Rew.* 19, 25-40.

[176] As demonstrated by recent revelations on NSA case, in the big data context people are not usually aware of being under surveillance. Only leaks of information can disclose these practices, open a debate on their legitimacy and give the chance to individuals to bring legal actions. See also European Parliament (2013). Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//EN> accessed 27 February 2014. On the role played by group actions in order to protect individual and collective interests concerning personal information, see Bygrave (n 52) 288-290.

[177] See also para 3.3.

[178] See art. 80 GDPR.

[179] For these reasons, a preventive approach based on risk assessment seems to be more effective than *ex post* legal actions. Moreover, it also contributes to tackle the risks of hidden forms of data processing, which often create an asymmetric distribution of the control over information in our society. See also Mantelero, A. (2014). Social Control, Transparency, and Participation in the Big Data World. *Journal of Internet Law*, April, 23-29.

In a digital economy based on a very short time-to-market, on the development of more than two thousand apps per day[180]and on an increasing number of IoT devices, there is a little room for a mandatory ethical and social impact assessment. This is indirectly demonstrated by the compromise reached about the DPIA, which largely remains an internal and non-publicly available assessment, with a low level of participation of the potential stakeholders.[181]

Against this scenario, the PESIA model is developed in this project as a voluntary solution. The aim of this project is to create a tool which may contribute to changing the existing paradigm and to suggest a different ethically and socially oriented development of digital devices.

At the same time, PESIA is not a standard. The definition of a standard needs a sufficient number of entities which are keen to adopt it, the convergence between the different actors in a given market and a specific entity entitled to maintain the standard. The variety of the IoT markets, the fragmentation of many sectors make it difficult to adopt a standard.

Moreover, the Virt-EU project does not aim to provide a sort of ethical or social check-list, but to enable data controllers (e.g. IoT developers) to have a clearer idea of the potential social and ethical implications of their data use. At the same time, controllers remain free to autonomously decide whether and how to address these implications

Finally, the PESIA adopts an open and participatory approach[182] and the outcome of this assessment can be publicly available. Therefore, the adoption of the PESIA model contributes to reinforcing data subjects' self-determination, as it makes explicit the dynamics of data uses, increases data subjects' awareness and facilitate their meaningful choices regarding data processing.

To reach these goals, the PESIA development has to address its main challenge, which is represented by the definition of the ethical and social values that are used in the assessment. Indeed, such a larger concern for the alignment of data use with ethical and social values implies a more complicated analysis than the traditional data protection assessment.

Whereas the driving values behind data security and data management are technology-based (e.g. integrity of data) and can therefore be generalised across varying social contexts, the situation with regard to social and ethical values is different. These are necessarily context-based and differ from one community to another, making it hard to pinpoint the benchmark to adopt for this kind of risk assessment.

---

[180] See Dogtiev, A. (2017). App Download and Usage Statistics. *Business of Apps*, November 21, 2017<http://www.businessofapps.com/data/app-statistics/> accessed 5 December 2017.

[181]A broad interpretation of the GDPR provisions on the DPIA has been recently provided by the Article 29 Data Protection Working Party, more favourable to a participatory and transparent DPIA, but there are many doubts about the effective capability to enforce these guidelines.

[182] In this sense, in literature, authors have supported participatory model against elitist approaches based on experts. See Otway, H. (1987). Experts, Risk Communication, and Democracy. *Risk Analysis*, 7(2), 125, 126 ("The view of decision making implicit in acceptable risk studies could be called technocratic, elitist, or maybe just "perfect-world" analysis, but it did nothing to further democratic process because the judgment of acceptability was seen as a matter for risk experts that we could tell people what was best for them").

To address this challenging scenario, the “architecture of values” that supports the PESIA model should be articulated on different levels. It should preserve a uniform baseline approach in terms of common values, but, at the same time, be open to the community traits and demands, as well as address the specific question posed by the societal impact of each given data processing.

For these reasons, the PESIA model will be based on three different layers of values. The first of them is represented by the common ethical values recognised by international charters of human rights and fundamental freedoms. This common ground can be better defined on the basis of the results of the ongoing analysis of the decisions concerning data processing adopted by the European courts (European Court of Justice and Europe Court of Human Rights).

The second layer takes into account the context-dependent nature of the social and ethical assessment and focuses on the values and social interests of given communities. Finding out these values is more difficult, since they are not codified in specific documents. Thus, the solution adopted in this project consists in analysing different sources that may provide a representation of the values characterising the use of data in a given society.

In the light of the above, the ongoing research on the PESIA values is focused on the analysis of the decisions adopted by data protection authorities in the European Union, trying to figure out the driving ethical and social values that may have underpinned the authorities’ decisions. This is not an easy task, since frequently the relevance of these values is not clearly affirmed in the decisions, whose authors prefer to use more formal legal arguments. Further sources to envisage the societal values at a community level may be the developers’ privacy practices as well as available ethical and privacy practical tools and frameworks.

Finally, the third layer of this architecture of values consists in a more specific set of values that can be provided by ad hoc committee with regard to the specific data processing application. These PESIA committees will act on the basis of the model of ethics committees, which already exist in practice and are increasingly involved in assessing the implications of data processing. In this sense the committees, whose nature and composition will be investigated in the second year of the project, should identify the specific ethical values to be safeguarded with regard to a given use of data, providing more detailed and context-based guidance for risk assessment.

5. Conclusions

With Articles 35 and 36 the EU legislator has created a model in which self-assessment (Article 35) and control of supervisory authorities are combined. Nevertheless, due to the manner in which these two elements are connected, this risk management model may be less efficient than expected.

The first stage (i.e. the DPIA) largely consists of an internal assessment, whose results are not compulsorily publicly available. In this regard, the guidelines provided by the Article 29 Data Protection Working seem to be an attempt by the Supervisory Authorities to mitigate this shortcoming and encourage controllers to take an

approach which is more oriented to data subjects' engagement and transparent assessment.

However, the weaknesses of the GDPR legal framework in terms of the participatory assessment and transparency of the DPIA, as well as the evident scarcity of Supervisory Authority resources point to the conclusion that the compromise reached in the GDPR is a missed opportunity to adopt stronger risk management models. Despite the potential fines for infringement of GDPR requirements (Article 83), there is a real risk that, in various countries, many controllers will prefer to underestimate the data processing risks and not seek prior consultation with the Supervisory Authorities for their processing operations.

Moreover, the DPIA only partially seems to address the main issues and challenges associated with data use. The focus on the potential risks of data processing has led the EU legislator, both in the Directive 95/46/EC and in the GDPR, to adopt provisions which are primarily focused on data security and data quality. They do not directly and broadly address the different social and ethical issues of data uses and do not provide a mechanism to assess the various possible negative outcomes for individuals and society.[183]

The increasing use of big data analytics in decision-making processes has heightened the need to take into account relations between individuals and society at large.[184] Potential harms are not restricted to the widely recognised privacy-related risks (e.g. illegitimate use of personal information, data security), but also include other prejudices, mainly concerning discriminatory or invasive forms of data processing.[185] This suggests that the existing Data Protection Impact Assessment should evolve into a broader and more complex Privacy, Ethical and Social Impact Assessment (PESIA).[186] The main challenge in developing this different model is represented by the definition of the social and ethical values which should be used to carry out the assessment. In this regard, the present deliverable suggests the adoption of a three-layer architecture that moves from a general level (internationally accepted values) to a more particular and case-specific level (values defined by local legal and community practices, PESIA committees).

The comparison between the DPIA and the PESIA points out the greater complexity of the latter and the additional burden it may place on companies or public bodies. However, there are cases in which a PESIA-like model may be favoured: ethically or socially oriented entities or developers' communities, sectors where the data subjects tend to pay greater attention to ethical and social implications of data use

---

[183] See Council of Europe, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data' (n 5), Section IV, para 2.3 ("Since the use of Big Data may affect not only individual privacy and data protection, but also the collective dimension of these rights, preventive policies and risk-assessment shall consider the legal, social and ethical impact of the use of Big Data, including with regard to the right to equal treatment and to non-discrimination").

[184] See also Raab, C. (2012). Regulating Surveillance: The Importance of Principles. In Ball, K., Haggerty, K. & Lyon, D. (eds) *Routledge Handbook of Surveillance Studies* (London; New York :: Routledge) 377–385; Raab & Wright (n 7) 363–383.

[185] See also The White House (2014). Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values <https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf> accessed 4 March 2017. See also Zarsky (n 154) 1560-1563; Wright & Raab (n 4).

[186] Definition of the PESIA model is still in its infancy; see the H2020 project "Virt-EU: Values and ethics in Innovation for Responsible Technology in Europe" <http://www.virteuproject.eu/> (accessed October 21, 2016).

(e.g. healthcare, services/products for kids), companies with an interest in the competitive value of fair data use.

Moreover, the emphasis of policymakers, industry and communities on the value of personal data as a key resource in the digital economy and the centrality of information to our society and the decision-making processes should stimulate a more responsible approach to data use. As it happens in other sectors chartered by innovation and potentially significant social risks, adequate forms of prior assessment may be adopted, at least in terms of best practices or soft-law.