Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Data protection, scientific research, and the role of information

*Rossana Ducato**

Postdoctoral researcher at UCLouvain and Université Saint-Louis – Bruxelles

ARTICLE INFO

Keywords:
Data protection
Scientific research purposes
Statistical purposes
Information duties
Transparency
GDPR
Law and behavioural science
Legal design

ABSTRACT

This paper aims to critically assess the information duties set out in the General Data Protection Regulation (GDPR) and national adaptations when the purpose of processing is scientific research. Due to the peculiarities of the legal regime applicable to the research context information about the processing plays a crucial role for data subjects. However, the analysis points out that the information obligations, or mandated disclosures, introduced in the GDPR are not entirely satisfying and present some flaws.

In addition, the GDPR information duties risk suffering from the same shortcomings usually addressed in the literature about mandated disclosures. The paper argues that the principle of transparency, developed as a "user-centric" concept, can support the adoption of solutions that embed behavioural insights to support the rationale of the information provision better.

1. Introduction

This paper aims to critically assess the information duties set out in the General Data Protection Regulation (GDPR) and national adaptations when the purpose of processing is scientific research. Due to the peculiarities of the legal regime applicable to the research context, information about the processing plays a crucial role for data subjects. However, the analysis points out that the information obligations (also known as mandated disclosures) introduced in the GDPR are not entirely satisfying and present some flaws.

In addition, the GDPR information duties risk suffering from the same shortcomings usually addressed in the literature about mandated disclosures. The paper argues that the principle of transparency, developed as a "user-centric" concept, can support the adoption of solutions which embed behavioural insights to support the rationale of information provision better.

The article is structured as follows. A preliminary issue to untangle is the definition of "scientific research" under the GDPR: what kinds of activities fall under this notion? What are the differences from neighbouring concepts, such as statistical purposes? (Section 2).

Once the boundaries of the concept of scientific research are clarified the applicable legal regime will be reconstructed. As will be shown in Section 3 the Regulation establishes a framework particularly favourable for research. Processing for such purposes can benefit from some exceptions to data protection principles and derogations to data subjects' rights. However, this special regime comes with obligations. Data

* Corresponding author: Address : UCLouvain, Faculté de droit et de Criminologie, Place Montesquieu 2, 1348, Louvain-la-Neuve (Belgium).
E-mail address: rossana.ducato@uclouvain.be

https://doi.org/10.1016/j.clsr.2020.105412

controllers, in particular, will have to set up appropriate measures and safeguards to protect the rights and freedoms of individuals. How these safeguards look is not entirely clear in either the adaptations of the GDPR or at the national level.

Section 4 will complete the analysis of the legal regime by investigating the lawful basis that can legitimise processing for research purposes. As the analysis will show, on the one hand data subjects' consent is not always necessary for processing and, on the other hand, research can open the door to secondary uses and indefinite retention of personal data originally collected for other purposes. Therefore, information duties established at Articles 13 and 14 GDPR remain a pivotal tool for data subjects to exert some form of control over their data.

However, mandated disclosures are a policy instrument that has been highly criticised in the literature.[1] In particular, they are unable to preserve the autonomy of the data subject for several reasons: people are decision-averse, data subjects suffer from a certain degree of illiteracy and innumeracy, readers are unable to cope with the overload and accumulation problem, and cognitive biases and heuristics interfere - often in unpredictable ways – with the decision-making process of individuals. In Section 5 such criticisms will be addressed and contextualised within the framework of the GDPR. In particular, identification of the potential shortcomings will be used to pave the way for viable interventions to effectively and dynamically inform data subjects. Such solutions, coupled with the controller's accountability duties, can help shape the abstract principle of transparency in practice and promote the data subject's *informationelle Selbstbestimmung*.

2. The notion(s) of research in the GDPR

The GDPR distinguishes between two main typologies of research: namely, historical and scientific research. Research purposes are then pooled in Article 89 GDPR with neighbouring scopes, such as archiving in the public interest and statistics. There being few differences between the four processing purposes from a normative standpoint, it is crucial to clarify the scope of application of each notion. This preliminary clarification is also functional for setting the context for the present paper since this contribution intends to focus specifically with the processing of personal data for scientific research.

2.1. *Historical purposes: distinguishing research from archiving in the public interest*

Historical research, scientific research, statistical and archiving purposes are not expressly defined in the body of the Regulation but spelt out in the recitals.

Processing for historical research purposes is not extensively defined in the GDPR. Recital 140 merely specifies that such processing includes "pure" historical research and research for genealogical purposes.

Historical research purposes have to be distinguished from archiving in the public interest. Differently from the situation under the Directive 95/46/EC, where historical research and archiving were combined by some Member States under the concept of "processing for historical purposes", the GDPR underlines the functional difference between the two.[2] Archiving in the public interest refers to services performed by public authorities or other bodies - both public and private - which have a legal obligation to "acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest"[3]. This will certainly include national and historical archives held by the State or public bodies but also those run by other cultural bodies whose archival mission is recognised under national law.[4] Archiving also includes activities carried out in order to provide "specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes"[5].

Therefore, archiving is a form of processing essentially consisting of the collection and permanent preservation of data and documents that is - eventually - prodromal to processing for historical research purposes.[6]

The conceptual difference between the purpose of historical research and archiving in the public interest is relevant from a normative perspective because the two are subject to different legal regimes. Where processing is for historical research Union law and Member States may introduce limitations to the rights of access (Article 15), rectification (Article 16), restriction of processing (Article 18) and object (Article

[1] *Ex multis*, Omri Ben-Shahar and Carl E Schneider, 'The Failure of Mandated Disclosures' (2011) 159 University of Pennsylvania Law Review 647; Omri Ben-Shahar and Carl E Schneider, *More Than You Wanted to Know. The Failure of Mandated Disclosure* (Princeton University Press 2014); Robert A Hillman, 'Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire?' (2006) 104 Michigan Law Review 837.

[2] It is the case of Italy. See, Giovanni Maria Uda, 'Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici' in Vincenzo Cuffaro, Vincenzo Ricciuto and Roberto D'Orazio (eds), *I dati personali nel diritto europeo* (Giappichelli 2019), p. 560 ff.

[3] Recital 158 GDPR.

[4] European Archives Group, *Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* (2018), p. 10.

[5] Recital 158 GDPR.

[6] What historical research and archiving in the public interest have in common is the express specification – made at recitals 158 and 160 – that the GDPR provisions do not extend to the data of deceased persons. This clarification seems superfluous given that the Regulation applies only to living natural persons (see recital 27). Perhaps it is merely a repetition that the legislator felt the need to stress in the historical context, where the collection of documents usually spans a prolonged period. However, it should be recalled that Member States remain free to regulate the processing of data relating to deceased persons. For an overview of the legal issues emerging in the context of "post-mortem" privacy the necessary reference is to Lilian Edwards and Edina Harbinja, 'Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world' (2013) 32 Cardozo Arts & Ent LJ 83; Giorgio Resta, 'La "morte" digitale' (2014) Diritto dell'informazione e dell'informatica 891; Edina Harbinja, 'Post-mortem privacy 2.0: theory, law, and technology' (2017) 31 International Review of Law, Computers & Technology 26.

21).[7] Meanwhile, if the purpose is archiving in the public interest, limitations can be introduced also with reference to the notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19) and the right to data portability (Article 20).[8]

2.2. *Scientific research and statistical purposes: a line in the sand?*

The concept of scientific research is introduced at recital 159 GDPR. The Regulation does not provide a definition but lists a series of examples, including "technological development and demonstration, fundamental research, applied research and privately funded research [...] studies conducted in the public interest in the area of public health"[9]. Scientific research is, therefore, any activity aimed at generating new knowledge and advancing the state of the art in a given field. Recital 159 expressly states that research must be interpreted "in a broad manner" under the GDPR.[10] The European Data Protection Board (EDPB), though, has affirmed that the concept should not be stretched beyond its common understanding. In particular, scientific research should refer to projects run "in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice"[11].

Notably, the notion of scientific research in recital 159 seems to include activities for profit, such as, for example, experimental development carried out by a company to improve or offer new services.[12] Moreover, reference to Article 179(1) TFEU confirms the importance of the private and industrial component in the context of scientific and technological development within the European Research Area.[13]

To complete the picture, the GDPR states that scientific research should include not only studies performed in the field of the so-called "hard sciences" but also research done in the humanities.[14]

Statistical purpose is defined as "any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results"[15]. The latter can be expressed in a numerical form (e.g., a percentage) or not (e.g., relationships may be established between the variables of an observed phenomenon or groups or categories identified based on common characteristics).[16] Data generated through a statistical process is, however, aggregated, meaning that the result cannot consist of data referable to a particular individual.

As for official statistics, further rules apply in addition to the GDPR. European statistics are subject to the provisions on statistical confidentiality set out at Article 338(2) TFEU and Regulation (EC) No 223/2009.[17] Analogously, official national statistics have to comply with the sector-specific domestic provisions.[18]

As for the secondary uses of statistical results, the GDPR makes it clear that the latter can be reused for other purposes, including for further processing for scientific research purposes (recital 163 GDPR). This clarification emphasises that statistical purposes are "other than" scientific research under the GDPR.

It must be said, though, that the boundaries between the two purposes are not clear cut. Considering the recommendations of the Council of Europe on statistical purposes, there are at least two features that are peculiar to statistical processing.[19] 1) Such processing aims at creating basic knowledge ("statistical knowledge is not an end in itself" [20]; "it usually serves other purposes"[21] among which is scientific research), and 2) statistical purposes exclude personalised impacts on individuals, i.e., the processing can result only in aggregate

[7] See Article 89(2) GDPR.
[8] Article 89(3) GDPR.
[9] Recital 159 GDPR.
[10] Ibidem.
[11] EDPB, *Guidelines on Consent under Regulation 2016/679 (wp259rev.01)* (2018), p. 27.
[12] EJ Kindt, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) 32 Computer Law & Security Review 729. Similarly, Viktor Mayer-Schonberger and Yann Padova, 'Regime change: enabling big data through Europe's new data protection regulation' (2015) 17 Colum Sci & Tech L Rev 315 (with reference to the processing for statistical purposes).
[13] However, some scientific organisations, such as the *Biobanking and BioMolecular resources Research Infrastructure - European Research Infrastructure Consortium* (better known as BBMRI-ERIC), have expressed serious concerns about the possibility that commercial entities might abuse of the preferential treatment reserved to scientific research by the GDPR, and have argued in favour of the application of Article 89 to research conducted in the public interest only. As reported by Mahsa Shabani and Pascal Borry, 'Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation' (2018) 26 European Journal of Human Genetics 149, p. 153.
[14] Recital 157 GDPR.
[15] Recital 162 GDPR.
[16] Council of Europe, *Explanatory Memorandum Recommendation No. R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes*, 1997, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806846ca, par. 9.
[17] Statistical confidentiality is defined as the "protection of confidential data related to single statistical units which are obtained directly for statistical purposes or indirectly from administrative or other sources and implying the prohibition of use for non-statistical purposes of the data obtained and of their unlawful disclosure" (Article 2(e), Regulation (EC) 223/2009). Confidential data used for the production of European statistics, in particular, may be processed by the National Statistical Institutes (NSIs), other national authorities and the Eurostat exclusively for statistical purposes, unless the data subjects in the survey sample have "unambiguously given [their] consent to the use for any other purposes" (Article 20(2), Regulation (EC) No 223/2009). However, the Commission, the NSIs and any other competent authority may authorise "access to confidential data which only allow for indirect identification of the statistical units [...] to researchers carrying out statistical analyses for scientific purposes" (Article 23(1), Regulation (EC) No 223/2009).
[18] Recital 163 GDPR.
[19] As indirectly suggested by the Council of Europe, *Explanatory Memorandum. Recommendation No.R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes* (1997).
[20] Ibid., points 14(a) and (b).
[21] Ibidem.

information with minimum interference with the individuals providing the data.[22]

Are these characteristics enough to draw a line between statistics and research? The first aspect (the creation of new knowledge) is unlikely to be decisive for a possible distinction. First of all, statistics is a scientific discipline that can be used in the research field. Like scientific investigation statistics also aims at generating new information and knowledge, through analysis of data about a collective phenomenon in a given cohort or population.[23] Such basic knowledge can be further used for other purposes, as results in basic science can later be exploited in applied science or technological development.

However, the second element (minimum interferences on individuals) can offer more grounds for grasping the distinction. As confirmed by recital 163 GDPR, in statistical processing both the result (output data) and the data used to generate that result (input data) shall not be used to take measures or decisions concerning any specific natural person.

This means, for example, that for statistical purposes the regime might apply to the activity of a company when it uses the personal data of its clients to develop a predictive model able to measure customers' abandonment rate.[24] In contrast, the same company will not benefit from the statistical purposes regime if the model identifies which customers may pass to competitors and automatically target them with special offers to make them stay.[25] Since the possibility of applying a statistical result to a particular person is excluded *a priori* by the law some authors have doubted the compatibility between the discipline of statistical purposes, envisaged at Article 89 GDPR, and profiling[26] or Big Data analytics in general.[27]

Concerning the results of scientific research, the GDPR is silent about whether they ought or ought not to have an impact on individuals. Hence, can the personalised intervention be an element for distinguishing the two purposes?

Comparative data does not offer a definitive answer. Statistics and research share a common core of principles, methodologies and aims that resonate in some national adaptations of the GDPR. Many Member States (Cyprus,[28] France,[29] Italy[30], Luxembourg,[31] Sweden,[32] UK[33]) have emphasised that neither processing for statistical or for research purposes can lead to personalised measures or decisions about particular subjects. Again, this specification is crucial because if processing has some consequences at the individual level the data controller will not benefit from the "favourable" regime provided for in Article 89 GDPR.[34]

Therefore, it can be stated that where the statistical or scientific processes are run to generate new knowledge without any specific impact on an individual Article 89 will generally apply. However, the exact boundaries of the notion of scientific research – including whether it can have an impact on individuals - are remitted to the Member States, with the risk of creating a fragmented framework at the European level.

3. The special regime for research purposes

Processing for research purposes enjoys a favourable regime within the GDPR, which seeks a balance in this field between the fundamental rights of individuals, the freedom to conduct

[22] Ibid., point 14(b).

[23] See also Article 3(1), Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities, OJ L87, 31 March 2009, p. 164-173.

[24] As suggested by Mayer-Schonberger and Padova, 'Regime change: enabling big data through Europe's new data protection regulation', p. 323.

[25] Ibidem.

[26] Ugo Pagallo, 'The legal challenges of big data: Putting secondary rules first in the field of EU data protection' (2017) 3 Eur Data Prot L Rev 36.

[27] Tal Zarsky, 'Incompatible: The GDPR in the age of big data' (2016) 47 Seton Hall Law Review 995. However, Member States still maintain a certain margin of discretion in regulating the "statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality" (recital 162 GDPR).

[28] Article 31, Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018), http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf. Such formulation resonates with the prohibition of Article 22 GDPR. "The processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be used for taking a decision which produces legal effects concerning the data subject or similarly significantly affects him or her".

[29] Article 4(2), Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460.

[30] Article 105(1), Italian Data Protection Code, https://www.garanteprivacy.it/codice (Italian only).

[31] Article 65(3), Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework, https://cnpd.public.lu/dam-assets/fr/legislation/droit-lux/Act-of-1-August-2018-on-the-organisation-of-the-National-Data-Protection-Commission-and-the-general-data-protection-framework.pdf.

[32] Section 3 of the Data Protection Act (Law 2018:218) provides that: "Personal data that is processed solely for research purposes may be used to take action regarding the data subject only if there are special reasons with regard to the data subject's vital interests". The individual use of personal data is considered an exception to the general rule of not processing data in the research context to take measures on specific individuals. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218 (Swedish only).

[33] Section 19(3), Data Protection Act, http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

[34] However, in the UK, an exception is provided for approved medical research. In that case the controller may enjoy the regime of Article 89 GDPR even if the processing could have a personalised consequence for the data subject. See, Section 19(3), Data Protection Act.

a business (recital 4) and the "legitimate expectations of society for an increase of knowledge" (recital 113).

The balance has been resolved as follows: if adequate safeguards for the rights and freedoms of data subjects are provided (Article 89.1) the GDPR designs a preferential regime aimed at facilitating research activities. Such a regime consists of, on the one hand, exceptions to some data protection principles (Article 5(1)(b); Article 5(1)(e); Article 9(2)(j) GDPR), and on the other hand derogations to the exercising of a set of data subjects' rights (articles 14, 15, 16, 18, 21 GDPR).

3.1. *Research as an exception to fundamental data protection principles*

The GDPR introduces three specific exceptions to fundamental data protection principles in cases of processing for the purposes enshrined at Article 89 GDPR. However, it is important to stress once again that these exceptions come into play as long as appropriate technical and organisational safeguards (art. 89.1 GDPR) are putted in place.

A first exception concerns the purpose limitation principle.[35] The GDPR establishes a presumption of compatibility[36] between (secondary) processing for research purposes and the original purpose of collection.[37] This exception is designed to simplify the rules for research and allow the re-use of personal data that are already lawfully collected. In this sense recital 50 confirms that the data controller may reuse data for research purposes, relying on the same legal basis as the initial processing.

A second exception regards the storage limitation principle.[38] The data processed for research purposes may be kept in a form which allows the identification of data subjects even beyond the period strictly necessary for the achievement of the purpose for which they were originally collected. This exception is particularly relevant in the context of scientific research, since the storage is fundamental to allow the verification of research results (so, even after the research project has officially ended). However, the EDPS has warned against the abuse of such provision: "the intention of the lawmaker appears to have been to dissuade *unlimited* storage even in this special regime, and guards against scientific research as a pretext for longer storage for other, private, purposes"[39].

The third exception concerns the special categories of personal data. As known, the processing of sensitive data is prohibited by default unless one of the conditions set out in Article 9(2) GDPR is met. Among these figures processing "necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"[40].

The wording of the provision is complex.[41] Trying to isolate the various elements, it can be said that: a) national or European law may authorise the processing of sensitive data b) provided that the processing is necessary for the achievement of the purposes referred to in Article 89 GDPR, and c) it is proportionate to the scope pursued. It is not entirely clear what is meant by the "essence of the right to data protection". In particular, whether it includes the core of principles set out in Article 8(2) of the Charter of Fundamental Rights of the EU (principles of fairness, purpose limitation, lawfulness, right of access and rectification) or the broader list contained in Article 5 GDPR.[42] However, the "appropriate and specific measures to protect the fundamental rights and the interests" of the data subject are likely to be guaranteed in addition to those provided for in Article 89(1) for the processing of "simple" personal data.[43]

3.2. *Research as a derogation to data subject rights*

The second order of favourable provisions for research comes from the restrictions that might be imposed on specific data subject rights. In Directive 95/46/EC Member States were allowed to introduce restrictions to data subjects' rights, provided that adequate safeguards were in place, the data were not used for taking measures or decisions against any particular individual, and there was no risk of breaching the privacy of the data subject.[44]

The GDPR is more articulated on this point. First of all, among the restrictions to the data subject rights it is possi-

[35] As known, the purpose limitation principle states that personal data may only be used for the specific, explicit and legitimate purposes for which they were obtained, and that they shall not be further processed for purposes incompatible with the original purpose of collection. See, Article 5(1)(b) GDPR and WP29, *Opinion 3/2013 on purpose limitation* (2013).

[36] Or a presumption of "non-incompatibility" as Article 5(1)(b) GDPR might suggest. See, Giovanni Comandé and Gianclaudio Malgieri, Guida al trattamento e alla sicurezza dei dati personali. Le opportunità e le sfide del Regolamento UE e del codice italiano riformato (Il Sole 24 Ore 2019).

[37] Article 5(1)(b) and recital 50 GDPR.

[38] Article 5(1)(e) and recital 65, GDPR.

[39] EDPS, *Preliminary opinion on data protection and scientific research*, 6 January 2020, p. 23.

[40] Article 9(2)(j) GDPR.

[41] As also underlined by the Belgian government in the document "Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) - Comments from Member States", 9 October 2019, available here: https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf. Belgium, in particular, submitted the following observations: "Specifically concerning Article 89.1 there appears to be contradiction between: Article 9.2 j) which states that scientific research needs to be accompanied by suitable measures based on EU or national law, and Article 89.1 which doesn't mention EU or national law".

[42] As pointed out by Comandé and Malgieri, *Guida al trattamento e alla sicurezza dei dati personali. Le opportunità e le sfide del Regolamento UE e del codice italiano riformato*. The case-law of the European Court of Justice seems to open the "essence" of the right to data protection to elements that are not mentioned in the wording of the Charter, and that might be considered "peripheral". As noted in *Digital Rights Ireland* (ECLI:EU:C:2014:238) by Orla Lynskey, *The foundations of EU data protection law* (Oxford University Press 2015), in particular, pp. 172-173.

[43] Comandé and Malgieri, *Guida al trattamento e alla sicurezza dei dati personali. Le opportunità e le sfide del Regolamento UE e del codice italiano riformato*.

[44] See, Article 13(2) Directive 95/46/EC.

ble to distinguish between derogations that are 1) laid down in the GDPR and 2) can be introduced by Union or Member States law.

Among the first group the GDPR provides for a limitation to the right to be informed. The latter, expressed in Articles 13 and 14, mandates the provision of a series of information duties to the data controller, who has to inform the data subject about the relevant aspects of processing, e.g., the identity of the controller, the purpose and legal basis used for the processing, transfer to extra-EU countries and appropriate guarantees, etc.[45] These information obligations represent a key tool for individuals in terms of controlling the flow of information related to them. Only if individuals are aware of processing and the relevant circumstances can they exercise the available data subject rights.[46]

However, *ad impossibilia nemo tenetur*, including the data controller.[47] When the provision of information proves impossible, requires a disproportionate effort or risks seriously compromising the achievement of the research the data controller is relieved of the information obligations provided for in Article 14, paragraphs 1 and 2.[48] This is not in any case a blanket exception and requires a balancing assessment. First of all, the "impossibility" and "disproportionate effort" must be tailored to "the number of data subjects, the age of the data and any appropriate safeguards"[49]. Second, the EDPB has further stressed the need for the controller to evaluate "the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information"[50]. This will consist at least of making the information publicly available (e.g. publication on website, newspapers, etc.)

It is important to bear in mind that such an exception applies only to information to be provided when the data are not directly obtained from the data subject. In contrast, the principle of transparency and information duties do not suffer any limitation when personal data are directly collected from the data subject. In other words, the legislator seems to have considered that the effort to inform from the beginning or to contact again later (in case of further processing for a different purpose) is presumed to be reasonable when the data controller has a direct relationship with the data subject. However, there might be cases where informing the data subject in a transparent way might compromise the achievement of the research.[51] This may happen, for example, in some experimental settings where the methodology would require to put in place some forms of covert surveillance or deception of the research participants. The practice is controversial and often discouraged by ethical committees, but it can be relevant in many contexts and for several disciplines (from ethnography to human-computer interaction). The EDPS has rightly encouraged a deeper debate on this point.[52] Nevertheless, it must be noted that, according to a purely literal interpretation, Article 13 leaves no space for imaging forms of "ex post" privacy notices.

The second set of limitations concerns the right to erasure when exercise of this by the data subject would render impossible or impair achievement of research purposes.[53] Subject to the conditions and guarantees set out in Article 89(1), the GDPR resolves the balance between conflicting interests in favour of research. Such a limitation to the right to erasure is justified in the light of the specific needs of the research context: erasure of whole or part of the data used for a study, even where technically possible, would risk undermining the scientific validity of research by preventing verification of its results and the *peer-review* process.

However, some authors have pointed out that the restriction to the right to erasure applies only to studies already concluded. [54] The right will remain intact, for instance, if data are stored for research purposes (according to Article 5(1)(e) GDPR) but not yet used in a project. After all, if the study has not yet begun exercising the right to erasure would not seriously be able to impair the achievement of the research goals.[55]

Another derogation expressly established by the GDPR is about the right to object. The latter can be invoked by the data subject for reasons connected to his or her particular situation only when processing is based on the legitimate interest of the controller. The GDPR, in contrast, prevents exercising the right to object in the context of research when the processing is necessary for the performance of a task carried out for reasons of public interest.[56] Therefore, before the superior interest of the public, the particular situation of an individual leading to an objection to processing can be limited by law.

Among the second group of derogations the GDPR expressly allows Union or Member States law to introduce limitations to the following rights: access (Article 15), rectification (Article 16), restriction of processing (Article 18) and to make objections (Article 21)[57]. Such limitations are permitted insofar as they are necessary and proportionate in a democratic society.[58] More specifically, the GDPR establishes a "three-step-test" for research derogations, centred on necessity and proportionality. To verify whether there are legitimate grounds for the introduction of exceptions to data subjects'

[45] The full list of mandated disclosures is contained in Articles 13 and 14 GDPR.

[46] For instance, the duty to inform ceases if the data subject already has the information. See Article 13(4) and 14(1)(a) GDPR. This is not an actual exception to the principle to inform the data subject. On the contrary, the principle of cognition is confirmed: the obligation ceases because the information is already within the data subject.

[47] See on this, EDPS, *Preliminary opinion on data protection and scientific research*, p. 20.

[48] As established by Article 14(5)(b) GDPR.

[49] Recital 62 GDPR.

[50] WP29, *Guidelines on transparency under Regulation 2016/679*, point 64.

[51] The issue has been pointed out recently by the EDPS, *Preliminary opinion on data protection and scientific research*, p. 21.

[52] Ibidem.

[53] Article 17(3)(d) GDPR.

[54] Kärt Pormeister, 'Genetic data and the research exemption: is the GDPR going too far?' (2017) 7 International Data Privacy Law 137, p. 140.

[55] Ibidem.

[56] Article 21(6) GDPR.

[57] As we have seen the right to object is already limited directly at Article 21(6) GDPR if the processing is necessary for the public interest. Therefore, the limitations that Member States can introduce are additional to Article 21(6) GDPR.

[58] See, in particular, recital 73 GDPR.

rights the following elements must be present cumulatively. First, exercising the rights is likely to render impossible or seriously impair the achievement of scientific purposes. Second, the derogations must be necessary for the fulfilment of those purposes. Finally, appropriate safeguards for the rights and freedoms of the data subject must be adopted. This latter point plays a crucial role in the balancing of interests. In the absence of the latter total implementation of all permissible derogations could lead to unwanted and unethical results.[59]

Interestingly, among the rights of the data subjects that Member States may derogate there is no mention of articles 20 (data portability) and 22 (automated decision-making process). These exclusions are certainly to be welcomed in the data subject perspective. They can be interpreted as a specific legislative choice to ensure the full fledging of data subjects' rights in these cases. However, the rationale for the exclusion of Article 22 from the derogations available to Members States could have a different explanation. In particular, it may derive directly from the definition of research and statistical purposes. If the goal of the latter is to produce new knowledge with no direct consequences for specific individuals, *a fortiori* scientific processing cannot end up with "decisions based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"[60]. Lacking the constitutive condition of the right enshrined at Article 22, it follows that a derogation to it cannot be foreseen in Article 89(2) GDPR.

4. The lawful basis for scientific research purposes

Although scientific research is by nature aimed at pursuing the general interest of society and advancing the state of the art of knowledge and applications in a particular field, such a purpose does not constitute *per se* a lawful basis for processing. With the only exception of Estonia, which has recognised research (and official statistics) as an autonomous legal basis alternative to consent,[61] the controller shall rely on one of the legal conditions listed in Article 6 GDPR. When processing concerns particular categories of data she shall also verify the fulfilment of one of the requirements provided at Article 9(2) GDPR.

Considering the possible lawful basis fitting for scientific research purposes, Article 6 offers three main roads: the consent of the data subject (Article 6(1)(a) GDPR), the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e) GDPR), or the legitimate interests of the controller or a third party (Article 6(1)(f) GDPR).

Considering the ethical aspects involved in research with human subjects, the most recurrent legal basis is usually represented by consent.[62] However, it has to be stressed that consent is just one of the possible lawful bases and is not even the most reliable option for the researcher, especially if she works with Big Data.[63] Data subjects have the right to withdraw their consent at any time (Article 7(2) GDPR). When they do so the lawful basis ceases to exist, and the researcher has to stop the processing of the data concerned immediately.

Therefore, data controllers are likely to rely on one of the other two mentioned lawful bases. On the one hand, they could do so if scientific research is recognised as a legal basis under Article 6(1)(e) GDPR.[64] This is, for example, the path opened by Finland.[65]

On the other hand, the legitimate interest of the controller or a third party could validly constitute a lawful basis for a research processing. The Article 29 Working Party suggested such a conclusion in Opinion 6/2014, where it affirmed that "the legitimate ground for these activities [research] will often be a well-considered use of Article 7(f) [Directive 95/46/EC]"[66]. Moreover, in light of the balancing test required by legitimate interest as a lawful basis, the drafting of recital 113 seems to weigh decisively in favour of third parties' interest when it states that "for scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration".[67] However, it must be recalled that the legitimate interest basis always requires a case-by-case evaluation that ponders the interests of the data controller and third parties, on the one hand, and the impact on data subjects, on the other hand. Therefore, assessment must be as granular as possible.

[59] As warned by Ciara Staunton, Santa Slokenberga and Deborah Mascalzoni, 'The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks' (2019) European Journal of Human Genetics 1.

[60] Article 22(1) GDPR.

[61] Section 6, Estonian Personal Data Protection Act Implementation Act, https://www.riigiteataja.ee/en/eli/523012019001/consolide. Section 6(3) lays down the appropriate safeguards and conditions for application. If the processing regards special categories of data research purposes remain a valid lawful basis. However, the competent ethics committee shall verify it. If there is no ethics committee in that area the task will be performed by the Data Protection Authority. See Section 6(4) Estonian Personal Data Protection Act Implementation Act.

[62] Paul Quinn and Liam Quinn, 'Big genetic data and its big data protection challenges' (2018) 34 Computer law & security review 1000. It is important to bear in mind that consent to the processing of personal data is conceptually different and, therefore, must be distinguished from the consent required for participation in research or clinical trials. See, Edward S Dove, 'The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era' (2018) 46 The Journal of Law, Medicine & Ethics 1013, p. 1022; EDPB, *Guidelines on Consent under Regulation 2016/679 (wp259rev.01)*.

[63] Comandé and Malgieri, *Guida al trattamento e alla sicurezza dei dati personali. Le opportunità e le sfide del Regolamento UE e del codice italiano riformato*; Quinn and Quinn, 'Big genetic data and its big data protection challenges', p. 1013.

[64] See also, EDPS, *Preliminary opinion on data protection and scientific research*, p. 23.

[65] Section 4, Finnish Data Protection Act, https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf.

[66] WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (2014), p. 28. Even though referring to Directive 95/46/EC, its recommendations are still valid for the legitimate interest basis in the GDPR.

[67] As noted by Shabani and Borry, 'Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation', p. 153.

In light of the principle of accountability the data controller must be able to justify its decision.

Concerning the processing of special categories of data for research purposes, a systematic interpretation of the GDPR leads to the conclusion that the condition laid down at Article 9(2)(j) is not *per se* a lawful basis for processing but an additional condition.[68] More precisely, it is an exception to the general prohibition concerning the processing of sensitive data in Article 9(1) GDPR. In other words, the conditions listed in Article 9(2) should not automatically set aside the applicability of Article 6, especially when this could lead to paradoxical results, i.e., when the processing of particular categories of data would be less protected than the processing of "simple" personal data.[69] Articles 9 and 6 should be applied cumulatively, as the drafting of recital 51 is likely to suggest: "in addition to the specific requirements for such processing [the reference is to the particular categories of data referred to in Article 9], the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing". The latter are precisely those mentioned at Article 6 GDPR.

Considering the number of exceptions to data protection principles and derogations to data subjects' rights when the purpose of the processing is scientific research, the role of information is key for data subjects to exert some form of control over the flow of personal data.

5. The role of information: an old problem in a new guise?

That information duties are a central pillar of data protection is one of those statements that are difficult to contest.[70] Since the moment when the concept of information privacy was reconstructed in terms of control over personal data[71] policymakers have found in the information to be given to data subjects the tool to 1) make people aware of the relevant aspects of processing, and 2) put them in a condition to act upon that knowledge.[72] The rationale behind this system is that by reducing information asymmetry through mandated disclosures the weak party (the data subject) is on a level playing field with all the other actors involved. Thus, the problem of loss of control is counterbalanced, and the data subject can efficiently exercise her right to information self-determination.

The paradigmatic moment when the data subject is called to make an informed choice is, for instance, when she has to consent to processing.[73] However, as we have seen, consent is not always required under the GDPR. Plus, data can be stored for longer periods and used for further research purposes. Therefore, when the processing occurs in the context of research the data subject might not be actively involved. In light of this, the information to be given to the data subject become a crucial tool for the data subject. Mandated disclosures can perform a fundamental function in the GDPR, for instance by allowing the data subject to know about their rights under Articles 15 ff and how to exercise them.

However, mandated disclosures have been highly contested in the literature, not only in the data protection domain but also in other fields where protection of the weak party has been delegated to information obligations, e.g., consumer protection or healthcare decisions.[74]

According to the fiercest critics of "disclosurism" information duties do not adequately enhance the self-determination of individuals due to a number of factors. First, because of the so-called "whatever argument"[75]. People are ontologically decision-averse. In most cases human beings tend to avoid, postpone, delegate a decision or choose based on a few elements. Making a choice that serves the interest of the individual is hard, and requires time, knowledge and effort.[76]

This problem is linked to the second one: privacy policies are usually long, difficult to read and make extensive use of techno-legal language, while the regular data subject suffers from various forms and degrees of illiteracy/innumeracy.[77] Therefore, even if data subjects are equipped with complete and accurate information the final result could frustrate the goal of disclosure.

A third issue concerns the quantity of information: disclosure can be simply too much (overload problem) or too much at once (accumulation problem).[78] In either case, lacking adequate expertise or experience the receiver will not be able to select and prioritise the information that is relevant to making a decision.

Finally, even when the individual conquers her natural decision-aversion, has readable and accessible information, and has the necessary skills and knowledge to understand them, other factors might come into play.[79] Notably, people are

[68] Dove, 'The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era'; Staunton, Slokenberga and Mascalzoni, 'The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks'; Mary Donnelly and Maeve McDonagh, 'Health Research, Consent and the GDPR Exemption' (2019) 26 European journal of health law 97.

[69] See, WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, p. 17-18.

[70] See, Gloria González Fuster, 'How uninformed is the average data subject? A quest for benchmarks in EU personal data protection' (2014) IDP Revista de Internet, Derecho y Política 92.

[71] On this, the necessary reference is to Alan F Westin, 'Privacy and freedom' (1968) 25 Washington and Lee Law Review 166.

[72] Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The perfect match? A closer look at the relationship between EU consumer law and data protection law' (2017) 54 Common Market Law Review 1427.

[73] Then it is true that in practice the way such a choice is presented can be misleading (e.g., the infamous examples of cookie banners or browsewrap agreements). However, this effect relates to poor implementation of the principle, rather than to the rationale of the principle itself.

[74] Ben-Shahar and Schneider, *More Than You Wanted to Know. The Failure of Mandated Disclosure*.

[75] Ibid. p. 59, ff.

[76] Moreover, individuals do not always decide rationally, as demonstrated since Amos Tversky and Daniel Kahneman, 'Judgment under uncertainty: Heuristics and biases' (1974) 185 Science 1124.

[77] Ben-Shahar and Schneider, *More Than You Wanted to Know. The Failure of Mandated Disclosure*, p. 79 ff.

[78] Ibid., p. 94, ff.

[79] Ibid., p. 107 ff.

not always the best connoisseurs of their situation or their interests. This statement may appear counterintuitive. However, it becomes clearer if we think, for example, about the privacy paradox: people tend to value privacy, but then they behave otherwise, e.g., they accept more privacy-intrusive options in exchange for free services (or supposedly so).[80] Furthermore, individuals have a problem of bounded rationality.[81] Human thinking works through heuristics and is affected by cognitive biases.[82] Therefore, it is prone to misinterpreting or misusing the most transparent disclosure. For instance, even if an individual receives accurate information about the risk of a particular transaction the bias of over-optimism or the "illusion of knowing" might lead people – not just the layman but even subjects supposedly more skilled, like entrepreneurs - to underestimate that information and to choose sub-optimally.[83] Considering that scholars have identified more than 200 biases and heuristics the rational decision-making process of an individual can be a minefield.[84]

The present contribution does not have the ambition of untangling the Gordian knot of disclosurism. However, a few points can be stressed and the relative consequences applied in the context of the GDPR. The goal is to show some potential inconsistencies *de lege lata* and shortcomings *de lege ferenda*, identifying promising lines of future investigation.

First of all, a general premise to frame the discourse is needed. Ending the use of mandated disclosure, would be difficult to implement in practice, at least in the European data protection domain. [85] Deleting Articles 13-14 GDPR would not automatically enhance the protection of the data subject, and problems concerning her decision-making process would remain. The removal of information obligations would require a comprehensive systemic change.[86]

Furthermore, the protection offered by the GDPR is not exclusively delegated to mandated disclosures. The latter are complemented by a system of check and balances, principles and remedies, technical and organisational safeguards, which in most circumstances protect individuals by default. Information duties are, therefore, just a piece of a broader framework.

Second, the apathy of the consumer towards disclosures has too often been overemphasised. Several studies have shown not only that the probability of reading increases if the information is displayed in a simple way[87] but also that consumers read and take into consideration the information when they are interested in it (e.g., for some kinds of contracts or they read it *ex post* if a problem arises).[88] The field of data protection has actually offered some notable examples of savvy readers that have challenged data controllers before courts.[89]

This general premise helps address, in particular, the above-mentioned "whatever argument" and the problem, often attributed to disclosure systems, of the excessive burden imposed on the weak party.

Finally, mandated disclosures are not a complete failure. In many cases, e.g., food labelling or consumer credit, they have proven to be effective.[90] However, whether the information obligations established in articles 13 and 14 GDPR fall within this positive trend is a matter that has to be verified empirically.

Therefore, the paper does not contest the existence of mandated disclosures in the GDPR as a policy tool but intends to critically examine whether careful implementation of such obligations that takes the principle of transparency seriously may address some of the concerns mentioned above. For the reasons already presented the first problem – the "whatever argument" – does not significantly affect the context of the

[80] The literature on the privacy paradox is vast. *Ex multis*, Alessandro Acquisti and Jens Grossklags, 'Privacy and rationality in individual decision making' (2005) 3 IEEE security & privacy 26; Patricia A Norberg, Daniel R Horne and David A Horne, 'The privacy paradox: Personal information disclosure intentions versus behaviors' (2007) 41 Journal of consumer affairs 100; Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and human behavior in the age of information' (2015) 347 Science 509; Spyros Kokolakis, 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon' (2017) 64 Computers & security 122.

[81] Ben-Shahar and Schneider, *More Than You Wanted to Know. The Failure of Mandated Disclosure*, p. 110 ff.

[82] Herbert A Simon, 'Models of man. Social and rational' (1957); Tversky and Kahneman, 'Judgment under uncertainty: Heuristics and biases'. More recently, Daniel Kahneman, *Thinking, fast and slow* (Macmillan 2011).

[83] Eric Van den Steen, 'Rational overoptimism (and other biases)' (2004) 94 American Economic Review 1141; Enrico Maria Cervellati Pierpaolo Pattitoni, Marco Savioli, 'Entrepreneurial underdiversification: Over optimism and overconfidence' (2013) The Rimini Centre for Economic Analysis Working Paper Series; Joshua Tasoff and Robert Letzler, 'Everyone believes in redemption: Nudges and overoptimism in costly task completion' (2014) 107 Journal of Economic Behavior & Organization 107.

[84] For an overview, a simple look here might give the sense of the magnitude of the problem: https://en.wikipedia.org/wiki/List_of_cognitive_biases.

[85] As suggested by Ben-Shahar and Schneider, *More Than You Wanted to Know. The Failure of Mandated Disclosure*.

[86] As observed in more general terms about European law by Geneviève Helleringer and Anne-Lise Sibony, 'European Consumer Protection through the Behavioral Lens' (2017) 23 Columbia Journal of Europen Law 607.

[87] Maartje Elshout and others, *Study on consumers' attitudes towards Terms and Conditions (T&Cs). Final report*, 2016; EU Commission, *Behavioural Study on the Transparency of Online Platforms*, 2018, https://ec.europa.eu/info/files/transparency-online-platforms-final-report-2018_en.

[88] Shmuel Becher and Esther Unger-Aviram, 'The law of standard form contracts: Misguided intuitions and suggestions for reconstruction', (2009) 8 DePaul Business and Commercial Law Journal 199; Shmuel Becher and Tal Zarsky, E-contract doctrine 2.0: standard form contracting in the age of online user participation' (2007) 14 Michigan Telecommunications & Technology Law Review 303.

[89] One might just mention the Schrems saga, inaugurated with C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650.

[90] Analogously in the field of consumer protection, see Helleringer and Sibony, 'European Consumer Protection through the Behavioral Lens'; Oren Bar-Gill, 'Defending (Smart) Disclosure: A Comment on More Than You Wanted to Know' (2015) 11 Jerusalem Review of Legal Studies 75.

present analysis. This contribution will now focus on the other three.

5.1. *Overload and accumulation problems*

When it comes to mandated disclosure one of the principal problems that data subjects have to face is the quantity of information about unfamiliar and complex decisions (overload problem).[91] Linked to this issue is the accumulation problem: all the disclosures compete for the – already limited – time and attention of the receiver. If information about how to lodge a complaint to the data protection authority can be crucial if something goes wrong, the provision of such information when data are obtained will not be that relevant and easy to forget.

These overload and accumulation problems go directly to the core of the mandated disclosures enumerated at Articles 13 and 14 GDPR and the timing established for the provision of that information.

As known, Article 13 GDPR contains a list of information obligations that the data controller has to provide when personal data are obtained directly from the data subject, while Article 14 details the information that has to be given when data are obtained from a third party. In the first case, the information must be provided at the time when personal data are obtained. In the second case, information has to be given: "a) within a reasonable period after obtaining the personal data, but at the latest within one month […]; b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed"[92]. The full list of mandated disclosures is reported in Table 1.

The first issue that catches the attention of the reader is the amount of information that the controller has to provide and the data subject to digest: an average of twenty pieces of disclosures. Some of them are specific to the context of collection. For instance, information about the categories of data obtained is mentioned at Article 14 only, since where personal data are directly collected from individuals the latter are actively providing the data and able to see what information is going to be processed. However, such an assumption is not always straightforward. In cases of automatic collection of personal data from an individual's device, sensors or cameras are such data collected from the data subject? According to the EDPB this kind of situation falls under Article 13 GDPR.[93] However, if this is the case then the data subject risks not being informed about the categories of data that will be transmitted by the device.[94]

Not all the information indicated in Articles 13 and 14 GDPR will always be present in a privacy policy. Some information is merely eventual: if there is no controllers' representative or no extra-EU transfer is envisaged the list will be shorter.

However, the critical issue with the mandated disclosures in the GDPR is not necessarily a quantitative one but a qualitative one. In Articles 13 and 14 GDPR the European legislator made a normative choice, establishing which information is relevant to know in any given processing. Nevertheless, the list is far from being complete, and the justification of some notable exclusions is not always easy to trace.

For example, as noted by Wachter, Mittlestadt and Russell, while the data subject has to be informed about her rights to access, rectification, erasure, restriction of processing and to object, Articles 13 and 14 do not mention the rights recognised at Article 22(3) GDPR, i.e., the right to obtain human intervention on the part of the controller, to express a point of view and to contest the decision.[95] Such a gap can undermine the information self-determination of the data subject: the latter will not be able to exercise those rights if she is not even aware of their existence.

Moreover, merely having information about the possibility of lodging a complaint with a supervisory authority might be inadequate for several reasons. First of all, the average data subject might not be familiar with the concept of a data protection authority, nor it can be reasonably expected that the data subject knows what the competent one is in her case. Many privacy policies available online state, for example, that the data subject has the right to lodge a complaint with the "leading supervisory authority", which is not necessarily the one where the data subject can legitimately complain. In fact, according to Article 77 GDPR, the data subject shall file the complaint "in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement". Furthermore, if it is not specified how to contact the supervisory authority this omission might deter the individual from acting. The cost of retrieving the information could represent an obstacle in practice. Austria[96] and Ireland[97], for example, have established in their national law the additional information duty to provide the data subject with the contact details of the supervisory authority.[98]

---

[91] Ben-Shahar and Schneider, *More Than You Wanted to Know. The Failure of Mandated Disclosure*, p. 101.

[92] Article 14(3) GDPR.

[93] WP29, *Guidelines on transparency under Regulation 2016/679* (2018), point 26.

[94] Interestingly Article 43(2)(4), Austrian Federal Act concerning the Protection of Personal Data states that: "In addition to the information referred to in para. 1, the controller shall give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights: […] Where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject". This case can potentially cover the information automatically collected by the controller. The statute can be accessed here: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html.

[95] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GPDR' (2017) 31 Harv JL & Tech 841.

[96] Article 43(1)(4) Austrian Federal Act concerning the Protection of Personal Data.

[97] Article 90(2)(e) Irish Data Protection Act (available here: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html).

[98] For instance, some DPAs recommend to indicate the contact details of the supervisory authority that individuals are most likely to complain to. See, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/.

Table 1 – List of mandated disclosure in the GDPR.

Article 13		Article 14	
1	the identity of the controller	1	the identity of the controller
2	the contact details of the controller	2	the contact details of the controller
3	where applicable, the identity of the controller's representative	3	where applicable, the identity of the controller's representative
4	where applicable, the contact details of the controller's representative	4	where applicable, the contact details of the controller's representative
5	the contact details of the data protection officer, where applicable	5	the contact details of the data protection officer, where applicable
6	the purposes of the processing for which the personal data are intended	6	the purposes of the processing for which the personal data are intended
7	the legal basis for the processing	7	the legal basis for the processing
	/	8	the categories of personal data concerned
8	where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party	9	where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party
9	the recipients or categories of recipients of the personal data, if any	10	the recipients or categories of recipients of the personal data, if any
10	where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	11	where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available
11	the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period	12	the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
12	the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability	13	the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability
13	where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal	14	where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
14	the right to lodge a complaint with a supervisory authority	15	the right to lodge a complaint with a supervisory authority
	/	16	from which source the personal data originate, and if applicable, whether it came from publicly accessible sources
15	whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract		/
16	whether the data subject is obliged to provide the personal data		/
17	the possible consequences of failure to provide such data		/
18	the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4)	18	the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4)
19	meaningful information about the logic involved if the processing is done accordingly to Article 22(1) and (4)	19	meaningful information about the logic involved if the processing is done accordingly to Article 22(1) and (4)
20	the significance and the envisaged consequences of the processing ex Article 22(1) and (4) for the data subject	20	the significance and the envisaged consequences of the processing ex Article 22(1) and (4) for the data subject

Moreover, considering the specific context of research, where Member States can limit some rights, there is no mention in the GDPR about the duty to inform of the lack thereof. Interpreting functionally the concept of the appropriate safeguards to be put in place by the controller according to Article 89(1) GDPR, information about the exceptions to data subjects' rights should be considered as one of those. However, even assuming a narrow interpretation of Article 89(1) GDPR (i.e., the appropriate safeguards refer exclusively to technical and organisation measures), if the controller has to inform about the existence of data subjects' rights it should respond to the principle of fairness to communicate when those rights have been restricted and why.

If we look at the national laws Belgium tackles this issue directly. Article 193 of the Belgian "Act on the protection of natural persons with regard to the processing of personal data"[99] establishes that when the controller collects personal data from a data subject for research purposes it has to inform her: "1. whether or not the data will be rendered anonymous; 2. *the reasons why the exercise of the rights by the data subject is likely to make the achievement of the purposes impossible or to hinder it seriously*". Meanwhile, when the data are collected from a third party the Belgian system implements an original measure imposing an information duty towards the other (former) controller. In a nutshell, the data controller that processes data for research purposes ("Controller 2") has to conclude an agreement with the original controller ("Controller 1"), or, where data are publicly available (or there is no other legal requirement to conclude the above-mentioned agreement) at least there is a duty to notify Controller 1. In both cases Controller 2 has to inform about the eventual restrictions on data subjects' rights. The underlying assumption of this model is that Controller 1 will act as a "contact point" for the data subject.[100]

In light of this, if a criticism can be raised about the content of mandated disclosures enshrined in Articles 13 and 14 GDPR it is that they do not necessarily cover the full spectrum of information that is relevant to the data subject. As just shown there are some notable flaws in the list. At the same time some information that has to be mandatorily given might not be relevant for data subjects. If the latter wants to complain about processing having a list giving contact details of the data controller, the representative, the data protection officer and the supervisory authority all at once may create confusion as to whom to address.

The list of mandated disclosures in the GDPR has been partially godfathered by Articles 10 and 11 of Directive 95/46/EC, with some important additions. However, it does not seem of having been accompanied by a comprehensive assessment or an empirical evaluation of the informative needs of data subjects. The conclusion emerging from the impact assessment of the GDPR proposal was that more mandatory information about processing was needed but without specifying why the chosen disclosures served the declared purpose of enhancing the protection of data subjects.[101]

The other issue with mandated disclosures in Articles 13 and 14 GDPR is about the accumulation problem and the timing of the provision of information.

On the one hand, a disclosure must be provided at the beginning (or according to the timing set up by Article 14(3) GDPR) and all at once. If this simplifies the obligations of the controller information fatigue is transferred entirely onto the data subject. The risk is continuing to confirm the stereotype of privacy policies as "paper tigers": instruments designed to protect the strong party rather than a tool for supporting in a functional way the rationale behind their conception. On the other hand, the GDPR does not address another critical issue, i.e. the timing of notifications in cases of changes concerning processing.[102] Therefore, some relevant information might be lost over the course of the the controller-data subject relationship.

In its guidelines on the principle of transparency the EDPB has underlined the tension between the goal to provide as complete information as possible and the need to make it meaningful for the data subject, as well as in terms of timing. Even though not formally binding the guidelines have a strong influence on how the GDPR has to be interpreted.

One possible solution that has been proposed in the EDPB document is to make information always available and accessible, while at the same time providing express reminders when a data subject might need the information.[103]

Furthermore, in order to address the overload and accumulation problem the EDPB suggests working on the modality for the provision of information, such as the use of layered notices.[104]

These recommendations and level of detail are not contained – and for obvious reasons – in the GDPR. However, they can be derived from the principle of accountability and the general duty of the controllers to provide "appropriate measures" to ensure the communication of transparent information.[105]

This behaviourally-informed approach supported in the EDPB guidelines can also pave the way for addressing the

[99] Belgian Act on the protection of natural persons with regard to the processing of personal data, https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Act_30_07_2018_final.pdf

[100] See, Articles 194 and 195, Belgian Act on the protection of natural persons with regard to the processing of personal data.

[101] See in particular Table 5, page 90 of COMMISSION STAFF WORKING PAPER IMPACT ASSESSMENT Accompanying the document 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) and Directive of the European Parliament and of the Council on the prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, https://ec.europa.eu/transparency/regdoc/rep/2/2012/EN/SEC-2012-72-2-EN-MAIN-PART-1.PDF.

[102] WP29, *Guidelines on transparency under Regulation 2016/679*, point 30. In any case, if the purpose of the processing changes (even if compatible with the previous one) data subject should be informed accordingly. See, EDPS, *Preliminary opinion on data protection and scientific research*, p. 20.

[103] WP29, *Guidelines on transparency under Regulation 2016/679*, point 34.

[104] A tool that has already been suggested in WP29, *Opinion 10/2004 on More Harmonised Information Provisions (2004) and* WP29, *Opinion 02/2013 on apps on smart devices* (2013).

[105] WP29, *Guidelines on transparency under Regulation 2016/679*.

other two problems mentioned in Section 5, i.e., the degree of illiteracy and innumeracy of data subjects and the problem of bounded rationality.

5.2. *The problems of the illiteracy and innumeracy of data subjects and bounded rationality*

If mandated disclosures are largely ineffective this may also depend on the educational and cognitive limitations of the data subjects themselves. While this argument can support the thesis about the failure of information duties, at the same time it suggests the way to overcome it.

Not all data subjects have a PhD in the several disciplines that it might be necessary to master in order to understand a privacy policy fully, and a data controller should reasonably be aware of it. Nevertheless, as a growing number of studies is demonstrating, privacy policies may be complex and require a high level of education to be deciphered.[106] Even when the reader is highly skilled and educated there is no insurance for the actual comprehension of a language that is often obscure (on purpose) and vague (inherently).[107]

The principle of transparency may offer a legal foothold for addressing the problem. This principle establishes that mandated disclosures about the processing must be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child"[108].

The open nature of such a clause requires further specification in practice. The already mentioned EDPB *Guidelines on Transparency* offer a first reading of such requirements, providing some useful example. So, for instance, the provision of intelligible information (Article 12 GDPR) means that information shall be "understood by an average member of the intended audience".[109] In other words, it would be possible to imagine a sort of "good (group) profiling". Since the data controller knows who her target is she could tailor the level of complexity of the information to be given. Evidently, the way information is provided to a group of legal experts has to be different from that given to teenagers.[110] Similarly, data subjects must be able to foresee the scope and consequences of processing, with particular regard to specific risks to data subjects' fundamental rights and freedoms.[111]

Concerning the requirement for "clear and plain language"[112], the EDPB enumerates a series of best practices. These include 1) information should be given in a simple and easy to understand manner, avoiding "complex sentence and language structures".[113] 2) Information should be unambiguous in the sense of not leaving room for different interpretations. 3) Vague formulas, like "may", might", "some" or "often" should be avoided (if used, the data controller has to demonstrate why it was not possible to be more precise). 4) The text should be clearly and logically structured (using bullets and indents). 5) The active form should be always preferred to the passive. 6) Highly technical or specialized language (including "legalese") should be avoided as much as possible. 7) In the case of multilanguage policy notices all linguistic versions must be consistent and clear. 8) A version in the data subject's language should always be available.

The second problem at stake here, i.e., bounded rationality, might be the most complex to address, however. The decision-making process of data subjects can be affected by countless biases, and properly preventing all of them would be a Sisyphean task. It must be said that not all heuristics and biases constitute a problem. Some mental shortcuts, even if not grounded in rationality, are useful and efficient in our daily life. The legally relevant question is rather how to recognise and defuse those biases that might produce negative consequences for individuals.

Some of these are already known, and legal safeguards have been put in place to combat them properly. For example, the inertia and status quo bias, which leads the decision-maker to stay with the default option, is fought by provisions that prohibit pre-ticked boxes for the collection of consent.[114]

Behavioural insights can contribute to fostering the recognition of such biases and the evaluation of their potential impact on the decision-making process of individuals. The law and behavioural science movement[115] or the legal design approach[116] could provide a suitable framework for incorporating behavioural insights into legally relevant arguments or actionable guidelines for policymakers, judges, and data controllers. Considering that knowledge about how heuristics and biases might alter the decision-making process of individu-

[106] Guido Noto La Diega, 'Grinding privacy in the Internet of Bodies. An empirical qualitative research on dating mobile applications for men who have sex with men'. In: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert (eds), Data Protection and Privacy: The Internet of Bodies (Hart 2018) 21; Rossana Ducato and others, *Protection of users in the platform economy: a European perspective*, forthcoming.

[107] Ben-Shahar and Schneider, *More Than You Wanted to Know. The Failure of Mandated Disclosure*, p. 84.

[108] Article 12(1) GDPR. See also recital 39.

[109] WP29, *Guidelines on transparency under Regulation 2016/679*, p. 9.

[110] Regarding information duties towards children, see also Ibid. p. 14, where the EDPB suggests using as a standard the "UN Convention on the Rights of the Child in Child Friendly Language".

[111] Ibidem.

[112] Article 12 GDPR.

[113] WP29, *Guidelines on transparency under Regulation 2016/679*, p. 12.

[114] See, for instance, Article 22 of the Consumer Rights Directive, recital 32 of the GDPR and the recent decision of the Court of Justice of the EU in *Planet49* (Judgement of the Court - Grand Chamber - of 1 October 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*, Case C-673/17, ECLI:EU:C:2019:801).

[115] Anne-Lise Sibony and Alberto Alemanno, 'The emergence of Behavioural policy-making: a European perspective'. In Alberto Alemanno and Anne-Lise Sibony, Nudge and the Law: A European Perspective, Hart Publishing (2015); Fabrizio Esposito, 'Conceptual Foundations for a European Consumer Law and Behavioural Sciences Scholarship'. In Hans-W. Micklitz, Anne-Lise Sibony and Fabrizio Esposito (eds), Research Methods in Consumer Law (Edward Elgar 2018) 38.

[116] Legal design can be defined as an "approach that applies human-centred design to prevent or solve legal problems" Rossana Ducato and others, 'The Legal Design Manifesto v. 1′ 2018) <www.legaldesignalliance.org> accessed 12 November 2019. See more in Margaret Hagan, *Law by Design* (2013), available here: http://www.lawbydesign.co/en/home/.

als is continuously growing,[117] the resulting insights could be used to support the introduction (or revision) of detailed information and transparency duties for controllers. One direction could then be to integrate behavioural insights into evidence-based policy. However, on a different side, if some empirical results enter the state of the art then they should be taken into account by a diligent controller in the designing of a privacy notice anyhow. If it is known in the literature that a kind of particular information framing can trick data subjects the data controller should at least adopt all appropriate measures to avoid that effect.

Opening up to behavioural studies and empirical insights in the field of data protection is not just a scholarly proposal. It is actually encouraged by the same EDPB. The group of data protection authorities makes a relevant point when they affirm that "the concept of transparency in the GDPR is user-centric rather than legalistic [...] The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR. However, the quality, accessibility and comprehensibility of the information are as important as the actual content of the transparency information, which must be provided to data subjects"[118]. Therefore, there is an express call for an interdisciplinary approach that could contribute to pursuing the legal rationale better. Thus, as part of the principle of accountability, the EDPB expressly invites data controllers to perform empirical evaluations to understand the level of transparency of the information directed to the data subject: "if controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/ notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things".[119]

This kind of experiment, which is at the core of law and behavioural science and legal design, can contribute to fixing the shortcomings experienced in the practice of mandated disclosures. If privacy notices were tested in labs and outside this would be decisive in bringing about better mandated disclosures, understanding what solutions work and in which contexts, identifying where information duties do not work, even if the information is communicated transparently, and proposing alternatives in order to integrate mandated disclosures with a broader arrangement of tools.[120]

6. Conclusions

This article has shed some light on the legal framework applicable to the processing of personal data for scientific research purposes. Despite the harmonisation intent of the GDPR scientific research is one of those areas where Member States can intervene with specific provisions. As the comparative overview has shown some divergences between national provisions have already emerged, even about the notion of scientific research itself. Although specification in light of the constitutional tradition of Member States concerning research is understandable some inconsistencies might nevertheless hinder the free flow of information across Europe, create legal uncertainties in cross-country research projects, and differentiate the level of protection of data subjects.

The reconstruction of the legal regime applicable to the research framework has contributed to pinpointing some moments in the chain of processing where the role of information emerges as a central tool for allowing a certain level of control by a data subject.

As shown, the relevant provisions (Articles 13 and 14) present some shortcomings in terms of content. Plus, the legislative intervention does not seem to have been grounded in empirical evidence. Although most of the disclosures in Articles 13 and 14 GDPR are reasonable, and it is easy to understand the aim of the addition, there are some important absences. For instance, there is no trace of the duty to inform about rights recognised at Article 22(3) GDPR in the case of solely automated decision processing.[121] The data subject must be informed about the possibility of lodging a complaint with a supervisory authority but then there is no obligation to show her how to to contact the competent supervisory authority. More dangerously, if data subjects' rights are restricted in accordance with Article 89(2) GDPR the data controller has no formal obligation to inform the data subject about that. To this end the paper presents the Belgian solution as a paradigmatic example that takes this aspect into account.

Another problem internal to the GDPR is about the lack of granularity concerning the provision of information. The latter has to be provided according to the rigid timing scheduled in Articles 13 and 14 GDPR but if there are relevant changes in the conditions of processing the GDPR is silent about the modalities and timing for that communication.

Finally, this paper has shown how the GDPR system could be open to the criticisms that are usually raised against mandated disclosures in general. However, it has been argued that the principle of transparency (Article 12 GDPR), as interpreted by the EDPB, is flexible enough to introduce and take advantages of behavioural insights. The latter can support the adop-

[117] The literature emerging on so-called "dark patterns" testifies to this trend. See, Christoph Bösch and others, 'Tales from the dark side: Privacy dark strategies and privacy dark patterns' (2016) Proceedings on Privacy Enhancing Technologies 237; Colin M Gray and others, 'The dark (patterns) side of UX design' (2018) Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 1; Ari Ezra Waldman, 'Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'' (2020). Articles & Chapters. 1332. https://digitalcommons.nyls.edu/fac_articles_chapters/1332; Arunesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 81.

[118] WP29, *Guidelines on Transparency under Regulation 2016/679*, p. 5.

[119] WP29, *ibidem*, p. 7.

[120] As suggested in the field of algorithmic explainability by Wachter, Mittelstadt and Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GPDR'; Kaminski, Margot E. and Malgieri, Gianclaudio, Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations (September 18, 2019). U of Colorado Law Legal Studies Research Paper No. 19-28. Available at SSRN: https://ssrn.com/abstract=3456224 or http://dx.doi.org/10.2139/ssrn.3456224.

[121] Wachter S, Mittelstadt B and Russell C, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GPDR'.

tion of solutions which can remedy the limits of mandated disclosures.

Acknowledgement

Rossana Ducato is supported by the Innoviris research grant 2016-BB2B-9.

The Author wishes to thank Fabrizio Esposito for the useful comments on an earlier version of this paper. The usual disclaimer about the maternity of the mistakes applies.

REFERENCES

Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information. Science 2015;347:509.

Acquisti A, Grossklags J. Privacy and rationality in individual decision making. IEEE security & privacy 2005;3:26.

Bar-Gill O. Defending (Smart) Disclosure: A Comment on More Than You Wanted to Know. Jerusalem Review of Legal Studies 2015;11:75.

Becher S, Unger-Aviram E. The law of standard form contracts: Misguided intuitions and suggestions for reconstruction. DePaul Business and Commercial Law Journal 2009;8:199.

Becher S, Zarsky T. E-contract doctrine 2.0: standard form contracting in the age of on-line user participation. Michigan Telecommunications & Technology Law Review 2007;14:303.

Ben-Shahar O, Schneider CE. The Failure of Mandated Disclosures. University of Pennsylvania Law Review 2011;159:647.

Ben-Shahar O, Schneider CE. More Than You Wanted to Know. The Failure of Mandated Disclosure (Princeton University Press 2014).

Bösch C. and others. Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proceedings on Privacy Enhancing Technologies 2016;2016:237.

Cervellati EM, Pattitoni P, Savioli M. 'Entrepreneurial under-diversification: Over optimism and overconfidence' (2013) The Rimini Centre for Economic Analysis Working Paper Series. Revised May 2016.

Comandé G, and Malgieri G. Guida al trattamento e alla sicurezza dei dati personali. Le opportunità e le sfide del Regolamento UE e del codice italiano riformato (Il Sole 24 Ore 2019).

Council of Europe. Explanatory Memorandum. Recommendation No.R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes; 1997.

Donnelly M, McDonagh M. Health Research, Consent and the GDPR Exemption. European journal of health law 2019;26:97.

Dove ES. The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law, Medicine & Ethics 2018;46:1013.

Ducato R. and others. Protection of users in the platform economy: a European perspective; forthcoming.

Ducato R. and others, 'The Legal Design Manifesto v. 1′ (2018) <www.legaldesignalliance.org>accessed 12 November 2019.

EDPB. Guidelines on Consent under Regulation 2016/679 (wp259rev.01); 2018.

Edwards L, Harbinja E. Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. Cardozo Arts & Entertainment Law Journal 2013;32:83.

Elshout M. and others, Study on consumers' attitudes towards Terms and Conditions (T&Cs). *Final report*, 2016.

EU Commission, Behavioural Study on the Transparency of Online Platforms; 2018, https://ec.europa.eu/info/files/transparency-online-platforms-final-report-2018_en.

Esposito F. Conceptual Foundations for a European Consumer Law and Behavioural Sciences Scholarship. In: Micklitz H-W, Sibony A-L, Esposito F, editors. Research Methods in Consumer Law (Edward Elgar 2018); 2018. p. 38.

Fuster GG. How uninformed is the average data subject? A quest for benchmarks in EU personal data protection. IDP Revista de Internet, Derecho y Política 2014:92.

Gray CM. and others. The dark (patterns) side of UX design others. ACM; 2018.

European Archives Group. Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector; 2018.

Hagan M., *Law by Design* (2013-ongoing).

Harbinja E. Post-mortem privacy 2.0: theory, law, and technology. International Review of Law, Computers & Technology 2017;31:26.

Helberger N, Borgesius FZ, Reyna A. The perfect match? A closer look at the relationship between EU consumer law and data protection law. Common Market Law Review 2017;54:1427.

Helleringer G, Sibony A-L. European Consumer Protection through the Behavioral Lens. Columbia Journal of Europen Law 2017;23:607.

Hillman RA. Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire? Michigan Law Review 2006;104:837.

Kahneman D. Thinking, fast and slow. Macmillan; 2011.

Kaminski M, Malgieri G. Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations (September 18, 2019). U of Colorado Law Legal Studies Research Paper No. 19-28. Available at SSRN: https://ssrn.com/abstract=3456224 or http://dx.doi.org/10.2139/ssrn.3456224.

Kindt E. Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. Computer Law & Security Review 2016;32:729.

Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security 2017;64:122.

Lynskey O. The foundations of EU data protection law (Oxford University Press 2015).

Mathur A. and others. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proceedings of the ACM on Human-Computer Interaction; 2019. p. 81.

Mayer-Schonberger V, Padova Y. Regime change: enabling big data through Europe's new data protection regulation. Colum Sci & Tech L Rev 2015;17:315.

Norberg PA, Horne DR, Horne DA. The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs 2007;41:100.

Noto La Diega G. Grinding privacy in the Internet of Bodies An empirical qualitative research on dating mobile applications for men who have sex with men. In: Leenes Ronald, van Brakel Rosamunde, Gutwirth Serge, De Hert Paul, editors. Data Protection and Privacy: The Internet of Bodies (Hart 2018); 2018. p. 21.

Pagallo U. The legal challenges of big data: Putting secondary rules first in the field of EU data protection. European Data Protection Law Review 2017;3:36.

Pormeister K. Genetic data and the research exemption: is the GDPR going too far? International Data Privacy Law 2017;7:137.

Quinn P, Quinn L. Big genetic data and its big data protection challenges. Computer law & security review 2018;34:1000.

Resta G. La "morte" digitale. Diritto dell'informazione e dell'informatica 2014:891.

Shabani M, Borry P. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. European Journal of Human Genetics 2018;26:149.

Sibony A-L, Alemanno A. The emergence of Behavioural policy-making: a European perspective. In: Alemanno A,

Sibony A-L, editors. Nudge and the Law: A European Perspective (Hart 2015); 2015. p. 1.
Simon HA. Models of man. Social and rational; 1957.
Staunton C, Slokenberga S, Mascalzoni D. The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. European Journal of Human Genetics 2019:1.
Tasoff J, Letzler R. Everyone believes in redemption: Nudges and overoptimism in costly task completion. Journal of Economic Behavior & Organization 2014;107:107.
Tversky A, Kahneman D. Judgment under uncertainty: Heuristics and biases. science 1974;185:1124.
Uda GM. Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In: Cuffaro V, Ricciuto V, D'Orazio R, editors. I dati personali nel diritto (europeo 2019). Giappichelli, 2019.
Van den Steen E. Rational overoptimism (and other biases). American Economic Review 2004;94:1141.
Wachter S, Mittelstadt B, Russell C. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GPDR. Harvard Journal of Law & Technology 2017;31:841.
Waldman AE. Cognitive Biases, Dark Patterns, and the 'Privacy Paradox' (2020). Articles & Chapters. 1332. https://digitalcommons.nyls.edu/fac_articles_chapters/1332.
Westin AF. Privacy and freedom. Washington and Lee Law Review 1968;25:166.
WP29. Opinion 10/2004 on More Harmonised Information Provisions; 2004.
WP29. Opinion 02/2013 on apps on smart devices; 2013.
WP29. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC; 2014.
WP29. Guidelines on transparency under Regulation 2016/679; 2018.
Zarsky T. Incompatible: The GDPR in the age of big data. Seton Hall Law Review 2016;47:995.

Author Information

Rossana Ducato is a postdoctoral researcher (chargée de recherche) at UCLouvain and Université Saint-Louis – Bruxelles, where she is carrying out the project "The Internet of Platforms. An empirical study on private ordering and consumer protection in the sharing economy". She is also lecturer and module leader of the Erasmus+ Jean Monnet course "European IT Law by Design", run at UCLouvain.