Author: Gianclaudio Malgieri, Jedrzej Niklas

Title: Vulnerable data subjects

Published in: Computer Law & Security Review Volume 37, July 2020,

Accessible at: https://doi.org/10.1016/j.clsr.2020.105415

The open access version of this research was funded by the EU Commission, H2020 SWAFS Programme, PANELFIT Project, research grant number 788039.

Available online at www.sciencedirect.com

ScienceDirect

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

Computer Law & Security Review

Vulnerable data subjects

Gianclaudio Malgieri[a,1], *Jędrzej Niklas*[b,1,*]

[a] *Vrije Universiteit Brussel, Belgium*
[b] *Cardiff University, United Kingdom*

ARTICLE INFO

Keywords:
Data protection
Vulnerability
Vulnerable groups
Discrimination
AI
Research ethics

ABSTRACT

Discussion about vulnerable individuals and communities spread from research ethics to consumer law and human rights. According to many theoreticians and practitioners, the framework of vulnerability allows formulating an alternative language to articulate problems of inequality, power imbalances and social injustice. Building on this conceptualisation, we try to understand the role and potentiality of the notion of vulnerable data subjects. The starting point for this reflection is wide-ranging development, deployment and use of data-driven technologies that may pose substantial risks to human rights, the rule of law and social justice. Implementation of such technologies can lead to discrimination systematic marginalisation of different communities and the exploitation of people in particularly sensitive life situations. Considering those problems, we recognise the special role of personal data protection and call for its vulnerability-aware interpretation. This article makes three contributions. First, we examine how the notion of vulnerability is conceptualised and used in the philosophy, human rights and European law. We then confront those findings with the presence and interpretation of vulnerability in data protection law and discourse. Second, we identify two problematic dichotomies that emerge from the theoretical and practical application of this concept in data protection. Those dichotomies reflect the tensions within the definition and manifestation of vulnerability. To overcome limitations that arose from those two dichotomies we support the idea of layered vulnerability, which seems compatible with the GDPR and the risk-based approach. Finally, we outline how the notion of vulnerability can influence the interpretation of particular provisions in the GDPR. In this process, we focus on issues of consent, Data Protection Impact Assessment, the role of Data Protection Authorities, and the participation of data subjects in the decision making about data processing.

* Corresponding author: Jędrzej Niklas, Cardiff University, United Kingdom.
E-mail addresses: Gianclaudio.Malgieri@vub.be (G. Malgieri), niklasj@cardiff.ac.uk (J. Niklas).

[1] Both the authors contributed equally to each paragraph. The authors would also like to thank the anonymous reviewer whose suggestions have greatly improved this article. The open access version of this research was funded by the EU Commission, H2020 SWAFS Programme, PANELFIT Project, research grant number 788039.

https://doi.org/10.1016/j.clsr.2020.105415
0267-3649/

1. Introduction

For decades, experts in research ethics have assumed that some research participants and communities are more likely to be mistreated, abused, exploited or harmed.[2] Such groups seem to possess a level of vulnerability, which generates certain obligations and responsibilities for researchers and oversight entities. The principle of special treatment of "vulnerable groups" was incorporated into various declarations and guidelines that regulate especially clinical research, like the Belmont Report or the Declaration of Helsinki.[3] Those documents predominantly focus on the issue of consent and informed participation, highlighting problems of autonomy and integrity. Nevertheless, some other interpretations add more elaborated understanding of vulnerability and raise issues of power imbalance and political and economic disadvantage.[4] In other words, the language of vulnerability in research ethics allows greater sensitivity and responsiveness to equity, discrimination and different socio-historical contexts. However, the notion of vulnerability is also discussed in other fields. From human rights to political philosophy, the concept is seen as a framework that enables the articulation of broad issues that fill into the category of social justice and *uncover human exposure to* harms, pain and suffering.[5]

As it will be argued below, human vulnerability is also (to some extent) present in the discussions about data protection, privacy and data-driven technologies. Calo, a prominent voice in this debate, argues that the rationale for privacy protection is precisely addressing vulnerability of individuals.[6] Put it differently, privacy and data protection regimes are manifestations of the idea that all individuals are vulnerable to the power imbalances created by data-driven technologies. Additionally, different scholars explain how data-driven technologies can lead to discrimination, social marginalisation or affect human autonomy and dignity and exploit particular communities.[7] Such controversial cases in the data-driven research concern automated systems that identify sexual orientation,[8] detect children anxiety and depression[9] or predict and prevent suicide.[10] Finally, the notion of vulnerability appears in the discussion about ethics and regulation of Artificial Intelligence. Here some of the guidelines and ethical policies call for the governance frameworks that recognise the situation of vulnerable groups such as women, persons with disabilities, ethnic minorities, children, and consumers.[11]

It seems to us that the issue of human vulnerability should be an important topic in the data protection debate, considering the new risks of individual exploitation in the algorithmic environment. Involving vulnerability as a "heuristic tool" could emphasise existing inequalities between different data subjects and specify in a more systematic and consolidated way that the exercise of data rights is conditioned by many factors such as health, age, gender or social status. However, the scholarly discussion about vulnerable data subjects is still largely underdeveloped. Accordingly, in this article, we try to understand and conceptualise how the notion of vulnerable individuals finds its way in the data protection debate. More precisely, when human vulnerability can influence the way we are interpreting data protection regimes.

We are aware that it is not possible to address this complex topic in one article satisfactorily. Our modest goal here is to initiate a discussion about this topic and its problematic aspects, suggesting some first interpretative paths, while calling for further analysis and research. To do this, we first investigate the meaning of "vulnerable individuals", looking in particular at the theoretical discussion about vulnerability (Section 2). Taking into account this background, in Section 3 we then review how data protection and the GDPR in particular address the position of vulnerable individuals. Building on these findings, we then try to understudy how the notion of vulnerability is present in other branches of EU

[2] Carol Levine et al., "The Limitations of 'Vulnerability' as a Protection for Human Research Participants," *The American Journal of Bioethics* 4, no. 3 (August 2004): 44–49, https://doi.org/10.1080/15265160490497083.

[3] Phoebe Friesen et al., "Rethinking the Belmont Report?," *The American Journal of Bioethics* 17, no. 7 (July 3, 2017): 15–21, https://doi.org/10.1080/15265161.2017.1329482.

[4] Dearbhail Bracken-Roche et al., "The Concept of 'Vulnerability' in Research Ethics: An in-Depth Analysis of Policies and Guidelines," *Health Research Policy and Systems* 15, no. 1 (December 2017): 8, https://doi.org/10.1186/s12961-016-0164-6.

[5] Lourdes Peroni and Alexandra Timmer, "Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law," *International Journal of Constitutional Law* 11, no. 4 (October 1, 2013): 1056–85, https://doi.org/10.1093/icon/mot042; Rebecca Hewer, "A Gossamer Consensus: Discourses of Vulnerability in the Westminster Prostitution Policy Subsystem," *Social & Legal Studies* 28, no. 2 (April 2019): 227–49, https://doi.org/10.1177/0964663918758513; Isabelle Bartkowiak-Théron and Nicole L. Asquith, "Conceptual Divides and Practice Synergies in Law Enforcement and Public Health: Some Lessons from Policing Vulnerability in Australia," *Policing and Society* 27, no. 3 (April 3, 2017): 276–88, https://doi.org/10.1080/10439463.2016.1216553, Martha Albertson Fineman, "The Vulnerable Subject: Anchoring Equality in the Human Condition," *Yale Journal of Law and Feminism* 20 (2008): 23; Judith Butler, *Precarious Life: The Powers of Mourning and Violence* (London ; New York: Verso, 2004).

[6] Ryan Calo, "Privacy, Vulnerability, and Affordance," *DePaul L. Rev.* 66 (2017): 592–593.

[7] For example: Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," *California Law Review* 671 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899; Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge: Harvard University Press, 2015); Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St Martin's Press, 2018); Ruha Benjamin, *Race after Technology : Abolitionist Tools for the New Jim Code* (Cambridge: Cambridge Polity Press, 2019).

[8] Yilun Wang and Michal Kosinski, "Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images.," *Journal of Personality and Social Psychology* 114, no. 2 (2018): 246–57, https://doi.org/10.1037/pspa0000098.

[9] Ellen McGinnis et al., "Giving Voice to Vulnerable Children: Machine Learning Analysis of Speech Detects Anxiety and Depression in Early Childhood," *IEEE Journal of Biomedical and Health Informatics* (2019): 1–2, https://doi.org/10.1109/JBHI.2019.2913590.

[10] Mason Marks, "Artificial Intelligence Based Suicide Prediction," *Yale J.L. & Tech. Special Issue*, 21 (2019): 98.

[11] See for example: High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019), 11 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58477>.

secondary law (Section 4). Acknowledging the limits of existing legislation and discussion, in Section 5, we finally propose a new vulnerability-aware interpretation of data protection law.

2. Theorising human vulnerability

The discussion about vulnerability has always had a multidisciplinary character. It emerged in a variety of fields, like political philosophy, gender studies, law, ethics and sociology. Very often, scholars from those different fields entered into dialogue with each other and adapted understanding of vulnerability developed in other areas (for example from political theory to bioethics). Our goal here is to demonstrate some seminal works that represent a variety of voices and at the same time help in grasping the crux of this debate. Throughout the whole article, we extensively refer to the legal literature on the problem of vulnerability. However, legal scholars have not yet fully developed the original approach to the notion of vulnerability. Most of them base their ideas on the work of theoreticians, especially Martha Fineman, who writes extensively about the relations between law, state and individual vulnerability. Presentation of those different theoretical approaches helps in placing the origins of this notion and its implications for institutions, legal systems and communities. Therefore, we found a theoretical introduction necessary for developing a vulnerability-aware interpretation of data protection.

Some early definitions and conceptualisation of vulnerability stressed its links to fragility, harms and the experience of being wounded, as its etymology suggests ('vulnus' in Latin means wound).[12] The term served almost as a synonym of dependency, helplessness, pain, violence and weakness.[13] As it was expressed by Goodin, "vulnerability implies more than susceptibility to certain sorts of harm … it also implies that the harm is not predetermined".[14] Accordingly, vulnerability refers to the potentiality of harm, not to actual harms occurred.[15] The concept of vulnerability has also been portrayed as a promising and alternative way to address injustices present in modern societies. For many scholars, vulnerability becomes a language to describe, e.g., social marginalisation, economic insecurity, precarious employment conditions or violence caused by wars. Fineman and Butler express that the concept has a great potential to challenge liberal individualism and redefine some of the existing frames about injustice, dependency or privilege.[16] While the field engaged in understanding the nature of vulnerability and explored its associations and consequences for political practice, ethics, research and law, the term is still deemed vague, complex and ambiguous.[17] However, some problematic dichotomies and uncertainties affect the application of the vulnerability concept in the institutional environment.

One of these dichotomies is between the *particular* and *universal* character of vulnerability. In more traditional approaches, vulnerability is a distinctive character of *particular* weaker individuals and groups, based on specific situations or socio-economic contexts.[18] Typical examples of such groups are racial minorities, asylum seekers, and people with disabilities. It is a predominant way of using the notion of vulnerability in more practical circumstances like research, social policy, or policing.[19] This way of understanding vulnerability was, however, accused of bringing stigmatising effects and harmful regulation for minorities.[20] For these reasons, some critical scholars reformulate the understanding of vulnerability as a *universal* human condition, which can change in different situations, different periods and also in spaces. The concept is portrayed as an ontological category and a general feature of human existence and embodiment.[21] However, some critics accuse that the emphasis of the universal character of vulnerability ignores structural violence, injustice and exploitation that are experienced by particular groups.[22] On the other hand, apologists of a universalised notion of vulnerability show this can be a way to run away from failures of existing diversity and equality policies and anti-discrimination laws.[23]

Another area of disputes about vulnerability concerns the organisational, legal and political responses to vulnerability. In this sense, vulnerability has a normative feature that involves specific actions, ethical judgments and institutional arrangements. For Goodin, vulnerability implies a justification for welfare state institutions that could help in addressing the lack of essential goods and services (in this sense, it has a clear distributive character).[24] In a similar tone, Fineman calls for re-

[12] Catriona Mackenzie, Wendy Rogers, and Susan Dodds, "Introduction: What Is Vulnerability, and Why Does It Matter for Moral Theory?," in *Vulnerability: new essays in ethics and feminist philosophy* (New York: Oxford University Press, 2013), 4–5, https://doi.org/10.1093/acprof:oso/9780199316649.003.0001.

[13] There are scholars who criticise only negative association of vulnerability, see for example: Erinn C Gilson, *The Ethics of Vulnerability: A Feminist Analysis of Social Life and Practice* (New York and London: Routledge, 2016) 7–8.

[14] Robert E. Goodin, *Protecting the Vulnerable: A Reanalysis of Our Social Responsibilities* (Chicago: University of Chicago Press, 1985), 112.

[15] Gilson, The Ethics of Vulnerability, 7–8.

[16] Fineman, "The Vulnerable Subject," 8; Butler, *Precarious Life,* 22–24.

[17] Peroni and Timmer, "Vulnerable Groups," 1058; Fineman, "The Vulnerable Subject," 9.

[18] Martha Albertson Fineman, "Beyond Identities: The Limits of an Antidiscrimination Approach to Equality," *Boston University Law Review,* 92, no. 6 (2012): 1750.

[19] For example: Hewer, "A Gossamer Consensus," 227–49; Nicole L. Asquith, Isabelle Bartkowiak-Théron, and Karl A. Roberts, eds., *Policing Encounters with Vulnerability.* (Cham: Springer International Publishing: Palgrave Macmillan, 2017).

[20] Alyson Cole, "All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique," *Critical Horizons* 17, no. 2 (May 3, 2016): 262, https://doi.org/10.1080/14409917.2016.1153896.

[21] Fineman, "The Vulnerable Subject," 23; Butler, *Precarious Life,* 26-28; Martha Nussbaum, *Frontiers of Justice : Disability, Nationality, Species Membership* (Cambridge: Harvard Univ. Press, 2006), 221.

[22] Frank Rudy Cooper, "Always Already Suspect: Revising Vulnerability Theory," *North Carolina Law Review* 93 (2014): 43; Cole, "All of Us Are Vulnerable, But Some Are More Vulnerable than Others," 260–77,

[23] Fineman, "The Vulnerable Subject," 18.

[24] Goodin, Protecting the Vulnerable, 145.

sponsive institutions and state architecture that recognise human vulnerability. She criticises existing systems of rights and laws that depend on the formal equality and embrace individualistic, self-sufficient and rationalist liberal subject. Fineman offers a different approach for the legal system and suggests a central role for "vulnerable subjects" in order to give institutional responses to context-specific dependences and injustices.[25]

Theorising in the field of bioethics, Rogers et al. explain that social practices and institutions can offer mitigation strategies toward vulnerability and encourage resilience.[26] Commentators in the research ethics field also stress that there are two ways of conceptualising and addressing consequences of vulnerability.[27] The first approach focuses on the harms and the ways to eliminate them.[28] The second approach focuses on individuals' ability to overcome their vulnerable position and empower them with various decisional and procedural safeguards. Put it differently, in one approach the emphasis is put on damages (physical or psychological), while in the second on consent or participation in the decision-making about the research process.

Those two problems discussed at the theoretical level (tension between universalistic and particular character of vulnerability and questions about vulnerability manifestation and related mitigation strategies) also have far-reaching consequences for the practical use of the vulnerability framework. However, some scholars have tried to conciliate these different views and to overcome dichotomies. One of them is Luna, who tried to reply to different criticalities through a new conception of vulnerability as *layers*. According to Luna, layers of vulnerability are not fixed attributes of specific individuals or groups but are features constructed by status, time and location. In this sense, the concept of layering provides an opening to a more intersectional approach and stresses its cumulative and transitory potential.[29] As Luna indicates, it is true that vulnerability is a universal condition of human beings, but it is also true that such condition of weakness may vary from an individual to another, may have different degrees of severity and many different factors.

We could summarise this universal-particular theory as follows: all individuals are vulnerable (there should be no labels on some groups), but some individuals have more layers of vulnerability than others. This is a consequence of different social contexts and relational balances.[30] The intensity of the legal protection of vulnerable individuals should be proportional to the quantity and quality of layers of vulnerability.[31] The identification and assessment of layers of vulnerability should be based on several criteria: an analysis of the origins of vulnerability (that is, an analysis of the stimulus conditions including if some layers are "cascade vulnerability", i.e. layers that have a cascade effect on other sources of vulnerability) and of its effects (that is, probability and intensity of harms).[32] Lastly, Luna's theory on layered vulnerability suggests that each vulnerability layer has its own mitigation measures. The obligations originated by layers evaluation (see above) should be: avoiding exacerbating layers, eradicating layers and minimising layers of vulnerability through different strategies (protections, safeguards, empowerment).[33]

In sum, the discussion about vulnerability is not singular and can lead to different paradoxes and dichotomies. Among the strengths of this discourse is a search for a more progressive conceptualisation of justice that is deeply rooted in human nature and different socio-historical contexts. Under this perspective, vulnerability may serve a ground for transformations of ethics, policy and law. At the same time, the relative vagueness and instability of this concept are its main weakness and create some serious challenges in its practical application. In this article, we argue that layered vulnerability can be one of the most suitable approaches to address those issues and the best response to several criticisms. More precisely, we will rely on the layers theory to understand vulnerability in the data protection field.

3. Situating vulnerable individuals in the data protection field

Building on these different theories and ways of understanding human vulnerability, we will now look at the notion of vulnerability in the data protection discourse and in particular in the GDPR. So far, vulnerability *per se* has not been a significant area of discussion among privacy and data protection scholars. However in our interpretation the notion plays a vital role in situating the position of the individual in the context of data processing. Nevertheless, at the same time we see that introduction of vulnerability in the data protection field may duplicate problematic dichotomies that we summarised in the previous section.

The first dichotomy relates to the definition of vulnerability in the field of privacy and data protection: there is a tension between particularistic and universalistic approaches. According to the universalistic approach, privacy and data protection safeguard all individuals equally in digital ecosphere, because we are all equally exposed to violations. As explained by Calo, knowledge and information confer power over individuals and make them vulnerable.[34] Therefore privacy and data rights play a protective function and create

[25] Fineman, "The Vulnerable Subject," 23.

[26] Wendy Rogers, Catriona Mackenzie, and Susan Dodds, "Why Bioethics Needs a Concept of Vulnerability," *International Journal of Feminist Approaches to Bioethics* 5, no. 2 (2012): 11–38, https://doi.org/10.2979/intjfemappbio.5.2.11.

[27] Doris Schroeder and Eugenijus Gefenas, "Vulnerability: Too Vague and Too Broad?," *Cambridge Quarterly of Healthcare Ethics* 18, no. 2 (2009): 18, https://doi.org/10.1017/S0963180109090203.

[28] Éloïse Gennet, Roberto Andorno, and Bernice Elger, "Does the New EU Regulation on Clinical Trials Adequately Protect Vulnerable Research Participants?," *Health Policy* 119, no. 7 (July 2015): 925–31, https://doi.org/10.1016/j.healthpol.2015.04.007.

[29] Florencia Luna, "Elucidating the Concept of Vulnerability: Layers Not Labels," *International Journal of Feminist Approaches to Bioethics* 2, no. 1 (2009): 121–39, https://doi.org/10.3138/ijfab.2.1.121.

[30] Ibidem.

[31] Ibidem, 86–95.

[32] Ibidem 92 and 93.

[33] Florencia Luna, "Identifying and Evaluating Layers of Vulnerability – a Way Forward," *Developing World Bioethics* 19, no. 2 (2019): 93, https://doi.org/10.1111/dewb.12206.

[34] Calo, "Privacy, Vulnerability, and Affordance," 594.

barriers for discovering, rendering and exploiting those vulnerabilities. However, in reality, the position of different data subjects is very diverse: they have different understandings, different levels of awareness, decisional capacity, propensity to disclose their data, and weakness. However, in the data protection discourse, the notion of data subject has generally been unique and rigid,[35] and there is no clarity about whether such unique notion refers to an average data subject (like in the consumer field) or not.[36] Scholars articulate how different situations of specific groups and individuals shape their capabilities, enjoyment and expectations about privacy and data protection. A typical example here is the situation of *children*.

Put it simply, children have limited capacity to understand the complexity of data-driven architecture, have less experience, less awareness of risks and rights and may be easily manipulated. For those reasons, processing data of minors is shaped by specific rules in data protection regimes and is also subject to numerous studies.[37] Nevertheless, the inequality between data subjects goes beyond the issue of age. In other contexts, scholars show that intrusion of privacy can be marked by social differences – race, ethnicity, class, sexual orientation, migration status or gender.[38] For example, those conditions very often act as a justification for particularly onerous forms of surveillance. Furthermore, Gilman argues that privacy laws are not always protecting those in less advantaged positions, mirroring existing inequalities and power dynamics.[39] Similarly, analysing the European context, Blume recognises that numerous factors like age, mental capacity, literacy or gender can affect the enjoyment and execution of individual data rights.[40]

In addition, we observe a distinction between vulnerability risks related to the *data processing* and vulnerability risks related to the *outcomes* of such data processing. Under the *first* perspective, vulnerability can emerge, for example, as the limited capability to provide free consent for collection of personal data, to understand information about data processing or to exercise data protection rights adequately. Those limitations may result from various factors like age, disability or socio-economic position.

Under the *second* perspective, vulnerability in the data protection framework emerges in the form of harms to which individuals are exposed. As explained by commentators, data-driven systems can serve as tools of potential discrimination, manipulation or may lead to physical and psychological harms. Different examples from law enforcement, welfare, banking or housing are showing that those technologies can reinforce social inequalities and lead to discrimination in the access to services and goods.[41] This discussion focuses very often on harmful biases embedded in models, training data and definitional problems.[42] Similarly, some controversial examples of data-driven research are accused of reproducing inflammatory stereotypes and creating life-threatening situations for specific marginalised communities.[43]

In sum, there are two major dichotomies in human vulnerability theories that we can find relevant also in the data protection discourse. One dichotomy concerns the definition of vulnerable subjects and is between universality (everyone is equally vulnerable) and particularity (some subjects are more vulnerable than others). The other dichotomy regards manifestations of vulnerability: vulnerability may arise within the data processing (decisional vulnerability risks related to data collection, consent provision, and inappropriate exercise of data protection rights) or as a consequence to the outcomes of the processing (some data processing may generate discrimination, manipulation or secondary harms such as physical or psychological harms).

Therefore, situating vulnerability in the data protection framework is a problematic task. If we affirm that all data subjects are universally vulnerable, we may ignore significant differences among them, which may weaken the protection of individuals in an already disadvantaged position. At the same

[35] Peter Blume, "The Data Subject," *European Data Protection Law Review* 1, no. 4 (2015): 259, https://doi.org/10.21552/EDPL/2015/4/4.

[36] Gloria González Fuster, "How Uninformed Is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection," *IDP Revista de Internet, Derecho y Política* 19 (November 2014): 92–104, https://doi.org/10.7238/idp.v0i19.2424.

[37] For example recent study by Mariya Stoilova et al. show different expectations and strategies employ to protect their privacy: Mariya Stoilova, Sonia Livingstone, and Rishita Nandagiri, "Children's Data and Privacy Online" (London: London School of Economics and Political Science, 2019).

[38] Mary Madden et al., "Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans," *Washington University Law Review* 95, no. 1 (2017); Khiara M. Bridges, *The Poverty of Privacy Rights* (Stanford: Stanford University Press, 2017) 1–35; John Gilliom, *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy* (Chicago: University of Chicago Press, 2001), 1–16.

[39] Michele E. Gilman, "The Class Differential in Privacy Law," *Brooklyn Law Review* 77, no. 4 (2012): 1394; Michele E. Gilman and Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization," *NYU Review of Law and Social Change* 42 (2018): 296–299.

[40] Blume, "The Data Subject," 258.

[41] Julia Angwin and Jeff Larson, "Bias in Criminal Risk Scores is Mathematically Inevitable, Researchers Say," *ProPublica*, December 2016, https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say; Virginia Eubanks, *Automating Inequality,* 1–13; Pasquale, *The Black Box Society,* 1–18; Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a 'right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review* 16, no. 1 (2017): 27–32, https://doi.org/10.31228/osf.io/97upg.

[42] For example Solon Barocas, "Data Mining and the Discourse on Discrimination," in *Proceedings of the Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining (KDD)* (New York, 2014), 4, http://www.cs.yale.edu/homes/jf/Barocas-Taxonomy.pdf; Danielle Keats Citron, "Promoting Innovation While Preventing Discrimination: Policy Goals for the Scored Society," *Wash. L. Rev.* 89 (2014): 1413; Oscar H. Gandy, "It's Discrimination, Stupid!," in *Resisting the Virtual Life: The Culture and Politics of Information*, ed. James Brook (San Francisco: City Lights Books, 1995), 35–47; Tal Zarsky, "Understanding Discrimination in the Scored Society," *Washington Law Review* 89, no. 4 (2014): 1375–1412, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2550248.

[43] Jacob Metcalf, "'The Study Has Been Approved by the IRB': Gayface AI, Research Hype and the Pervasive Data Ethics Gap," *Medium* (blog), 2017, https://medium.com/pervade-team/the-study-has-been-approved-by-the-irb-gayface-ai-research-hype-and-the-pervasive-data-ethics-ed76171b882c.

time, more specific protection rules and safeguards can lead to fragmentation of the already complicated legal regime. Also, while focusing on harms, the discussion could easily end up with a never-ending list of damages, which are not providing any additional value. On the other hand, concentrating on procedural safeguards can neglect the importance of actual damages, suffer and pain that some individuals may experience as a result of the use of particular data-driven technologies. Those problems may lead to the conclusions that vulnerability in the data protection framework can be a dead end, but – as we argue below – there is at least one theory that could help develop the notion of data subjects' vulnerability in a constructive way. We refer to Luna's theory of layered vulnerability (see below).

3.1. *Data subjects' vulnerability in the General Data Protection Regulation*

In order to better understand what the notion of individual vulnerability in the GDPR is and why a layered approach to vulnerability might be a constructive step further, we will now analyse the wording of the GDPR and the interpretations offered by the Article 29 Working Party (WP29) and the European Data Protection Board (EDPB). As we affirmed in the previous section, when dealing with the notion of vulnerable subjects there are two dichotomies to address: definition (universalism versus particularism) and manifestations (vulnerability *within* the data processing versus vulnerability *to the outcomes* of the processing).

The first dichotomy to consider regards the definition: what is the status of a vulnerable person in the GDPR and how could we eventually solve the dichotomy between universal and particular vulnerability interpreting the wording of the GDPR? Actually, the GDPR does not contain an explicit definition of vulnerable data subjects. There is just one slight reference in recital 75 about relevant risks to consider when performing a Data Protection Impact Assessment: "where personal data of *vulnerable natural persons, in particular of children*, are processed". "In particular" means that children are vulnerable subjects, but that also other data subjects might be considered vulnerable. The situation of children is specifically addressed in the GDPR – through requirements for consent for information society services (Article 8) and specific transparency duties towards children (Article 12(1).[44]

Considering that children are specifically vulnerable data subjects, one may conclude that the GDPR approach to vulnerability is *particular* and not universal: just some groups (namely, children) are vulnerable. However, the definition of the data subject – as already affirmed – is universal and unique[45] and children are just one group at high risk, but other groups can usually have similar risks (for example: elderly, mentally ill persons).

Importantly, the GDPR offers at recital 38 a justification for this special protection for children: "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data". In other words, a lack of awareness and understanding about consequences and legal rights (what we can call decisional vulnerability) justifies the particular protection for children. The idea of decisional vulnerability of children is then reaffirmed at recital 65 that emphasises the problem of consent in the context of erasing personal data. Additionally, recital 58 reveals that the reason for protection is mainly based on children's reduced capacity of understanding. However, one may wonder whether some of the rationales for the protection of children in the data protection framework can be considered – by analogy – also for other vulnerable adults. Although the answer is not clear, WP29 has provided some guidance on this matter and it remarked in several opinions that vulnerability could not be limited only to children.

In particular, WP29 argues that the key factor in identifying individual vulnerability is a power imbalance between the data subject and the data controller. Power imbalance means that individuals may be "unable to easily consent to, or oppose, the processing of their data, or exercise their rights". WP29 tries to enlist some vulnerable data subjects: children, since "they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data"; employees; more vulnerable segments of the population requiring special protection ("mentally ill persons, asylum seekers, or the elderly, patients, etc."), and "in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified".[46] Here the link between *power imbalance* and *vulnerability* of the data subjects is clear: when the data controllers are in a position of significant power imbalance (in particular in terms of possible impacts on fundamental rights and freedoms, significant information asymmetry based on predictive analytics, etc.) towards the data subject, the latter should be considered vulnerable.

[44] About the topic of children data protection see, in general, Lina Jasmontaite and Paul de Hert, "The EU, Children under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet," *International Data Privacy Law* 5 (2014): 20–33, https://doi.org/10.1093/idpl/ipu029; Alessandro Mantelero, "Children Online and the Future EU Data Protection Framework: Empirical Evidences and Legal Analysis," *Int. J. Technology Policy and Law* 2 (2016): 169–81, https://doi.org/10.1504/IJTPL.2016.077189; Eva Lievens and Valerie Verdoodt, "Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation," *Computer Law & Security Review* 34, no. 2 (2018): 269–78, https://doi.org/10.1016/j.clsr.2017.09.007; S. van der Hof, "I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World," *Wisconsin International Law Journal* 34, no. 2 (2017): 409–45; van der Hof Simone and Eva Lievens, "The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR," *Communications Law* 23 (2018), https://papers.ssrn.com/abstract=3107660.

[45] See Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, 21–22.

[46] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 10.

Similar wording can be found in the WP29 Opinion on legitimate interests.[47] When data controllers perform the balancing test that is required if they want to process personal data on the basis of legitimate interests (Article 6(1)(f) of the GDPR), they need to consider the nature and source of the legitimate interest, if there are additional safeguards and what is the impact on the data subject, considering in particular "the status of the data controller and data subject, including the *balance of power between the data subject and the data controller*, or whether the data subject is a child or otherwise *belongs to a more vulnerable segment of the population*."[48] Again, the idea of vulnerability is linked to power imbalance. In particular, vulnerability is considered as a contextual notion: "the question whether the data subject is an employee, a student, a patient, or whether there is otherwise an imbalance in the relationship between the position of the data subject and the controller must certainly be also relevant. It is important to *assess the effect of actual processing on particular individuals*."[49] Similar views were articulated in the WP29 Guidelines on Purpose Limitation under the Data Protection Directive and WP29 Guidelines on Transparency.[50]

WP29 has also expanded the notion of vulnerable groups beyond children, when addressing the meaning of "significant effects" under article 22, GDPR. In that opinion, WP29 clarifies that when assessing the effects of automated decisions on individuals, one factor to be considered is whether the controller used "knowledge of the vulnerabilities of the data subjects targeted".[51] The notion of vulnerability is very much related to adverse impacts: "processing that might have little impact on individuals generally may in fact have a significant effect for certain groups of society, such as minority groups or *vulnerable adults*".[52]

As regards the other dichotomy, i.e. the manifestation of vulnerability within the data processing or as an outcome of the data processing, it seems that WP29 addresses both aspects. The analysis of children vulnerability focuses predominantly on the processing side (i.e. decisional vulnerability related to the collection of data, to the provision of consent and to the exercise of data subject rights).[53] However, in the Guidelines on Data Protection Impact Assessment, the vulnerability of data subjects is considered one of the nine indexes for identifying cases of high risks of data processing under Article 35 GDPR.[54]

Recital 75 suggests the reason why vulnerable data subjects (in general, not only children) require special attention when determining whether a data processing is of high risk for rights and freedoms of natural persons. Those risks "may result from personal data processing which could lead to physical, material or non-material damage, in particular (…) where personal data of vulnerable natural persons, in particular of children, are processed".[55] In other words, some subjects should be protected not only because of their limited capacity to understand and give consent, but from higher risks of material or non-material damages. The examples might be several: some subjects are more at risk of discrimination during an automated data processing (in particular in case of, e.g., automated profiling); other subjects might be more easily impaired in their freedom of thought when their data are processed for direct marketing; other subjects might have bigger physical or psychological damages in case of a data breach, etc. Children are a category that is both decisionally vulnerable and is exposed to the higher risks of harms. However, we can easily imagine categories of data subjects who have no reduced decisional capacity but can suffer from higher risks of damages from a data processing.

In sum, we preliminarily analysed the definition of vulnerable subjects and the manifestations of vulnerability in the GDPR. In both these areas, we observe dichotomies: as regards the definition of vulnerable individuals, there is a tension between a universal notion of vulnerability (since there is no reference to vulnerable groups and just an open reference to vulnerability in recital 75) and a particular one (just children are mentioned as an example and there are specific safeguards only for children). However, it seems that the GDPR is open to both approaches: particularism and universalism. As we will argue in the final sections, the solution to this apparent contradiction is in the notion of "risk", which is very close to Luna's notion of "layers" of vulnerability. The risk-based approach in the GDPR suggests a layered analysis of vulnerability, i.e. everyone is potentially vulnerable, but at different levels and in different contexts.

As regards the manifestation problem, vulnerability risks *within* the data processing itself (i.e. decisional vulnerability related to data collection and the lack of capability to exercise data rights) are the declared rationale for protecting the only explicit vulnerable category (i.e. children). However, recital 75 and WP29 emphasises more on vulnerability risks arising as an *outcome* of the data processing.

In order to better solve these apparent contradictions, the following section will investigate the understanding and scope of individual vulnerability in the international human rights law and the EU law. To do that, we will look both at the European Convention on Human Rights (and the relevant caselaw of the ECtHR) regarding vulnerable individuals and at the EU law to understand if we can profit from more developed notions of vulnerability. In particular, we will observe whether the approach is to propose a specific list of vulner-

[47] Article 29 Working Party, Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC".
[48] Ibidem, 51.
[49] Ibidem, 41. Emphasis added.
[50] Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, 32; Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679" clarifying requirements of the EU GDPR, WP 260, 9.
[51] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251 rev.01, 22.
[52] Ibidem, 22.
[53] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 10.
[54] Ibid.
[55] See Recital 75, GDPR.

able groups or assuming an open clause for a universal notion of vulnerability. Also, we will see whether vulnerability manifestations are focussed more on decisional vulnerability or to risks of subsequent harms.

4. The broader perspective: vulnerability in the EU law

4.1. *Vulnerability and human rights: the rise of the concept of vulnerable persons in the ECtHR jurisprudence*

The notion of vulnerability plays a significant role in the human rights discussion. Although the concept of vulnerability is neither present in the European Convention on Human Rights nor the EU Charter of Fundamental Rights, scholars and human rights institutions and organisations refer to it as an imperative that entails special protection of socially marginalised groups like women, people with disabilities, children, or ethnical minorities.[56] The ECtHR recognises vulnerable situations of particular groups, but it never employed the notion of vulnerability in the field of private life, privacy or data protection (Article 8 ECHR).

The Court has firstly addressed the idea of vulnerable persons in 1981, referring to children. In *Dudgeons v. UK*[57] the Court referred to "the moral interests and welfare of certain individuals or classes of individuals who are in need of special protection for reasons such as *lack of maturity, mental disability or state of dependence*".[58]

In this judgment, the Court adopted the idea of *inherent vulnerability* based on (*age* as an index of) weakness, inexperience and dependence.[59] In particular, the category of children vulnerability qualifies as intrinsically gradual and temporal. However, the Court tends to assume a hybrid definition of vulnerability, both *universal* and *particular*, as the wording "specially vulnerable" reveals: all individuals are potentially vulnerable, but some are especially vulnerable.[60]

In later judgments, the ECtHR extended the notion of vulnerability to politically and socially disadvantaged groups. For example, in *Chapman v. The United Kingdom* the Court stated that "the vulnerable position of Gypsies as a minority means that some special consideration should be given to their needs and their different lifestyle both in the relevant regulatory planning framework and in reaching decisions in particular cases".[61] The category of vulnerable groups was also expanded to asylum seekers, people living with HIV and individual facing social disadvantage and material deprivation.[62] The partly dissenting opinion of Judge Salò has critically developed the definition of vulnerable persons under the ECtHR jurisprudence. He originally observes that the concept of vulnerability is not a monolith, there are different grades of vulnerability based on different situations.[63] Those different cases show also that the Court perceives vulnerability as relational, harm-based and depending on the situation of particular communities, ethical groups or life situations.[64]

The reference to vulnerability in the ECtHR jurisprudence also has three significant legal consequences.[65] Firstly, vulnerability requires establishing positive obligations toward disadvantaged groups and providing tailored measures that recognise their particular needs and situations. For example, in *Chapman* case the Court called British authorities to acknowledge the situation of Roma in the policymaking process.[66] In other cases, the Court obliged governments to provide special financial assistance to asylum seekers or shelter to people who were evicted by force.[67]

Secondly, vulnerability of particular groups can also influence the weight of harm in the proportionality test, amplifying the consequences and scope of harms. As stressed in the *Yordanova* case: "the applicants' specificity as a social group and their needs must be one of the relevant factors in the proportionality assessment that the national authorities are under a duty to undertake".[68]

The third consequence is related to the margin of appreciation. As it was explicitly mentioned in the *Kiyutin v. Russia* case, in the situation of vulnerable groups: "State's margin of appreciation is substantially narrower, and it must have very weighty reasons for the restrictions in question".[69]

Vulnerability is a central and vital aspect of human rights legal practice. It helps understand the particularity of certain disadvantaged groups and understand that economic, historical and social conditions play an important role in the enjoyment of rights. Therefore, the recognition of vulnerability allows to acknowledge problems of discrimination, procedural safeguards, distributional policies or political participation. Such approach links vulnerability in the human rights discourse to the broader problems of social justice. This contrasts with the conceptualisation of vulnerability in other fields (i.e. research ethics) that focus predominantly on consent and other decisional aspects.

4.2. *The rise of vulnerable individuals in the EU secondary law: an overview*

While vulnerability emerges somehow "naturally" in the human rights field, other fields of law refer to it as well. Although

[56] See in general Francesca Ippolito and Sara Iglesias Sánchez (Ed.), *Protecting Vulnerable Groups: The European Human Rights Framework* (Bloomsbury Publishing, 2015); See also, in the US discourse Bryan S. Turner, *Vulnerability and Human Rights* (University Park: Pennsylvania State University Press, 2006).

[57] *Dudgeons v. UK*, Application no. 7525/76, (22 October 1981).

[58] Ibidem, §47. Emphasis added.

[59] Francesca Ippolito, "(De)Constructing Children's Vulnerability under European Law," in *Protecting Vulnerable Groups*, 23–48.

[60] Peroni and Timmer, "Vulnerable Groups," 1056–85.

[61] *Chapman v. The United Kingdom,* Application no. 27238/95, (18 January 2001), §95.

[62] *M.S.S. v. Belgium and Greece*, Application no. 30696/09, (21 January 2011); *Kiyutin v. Russia*, Application no. 2700/10, (10 March 2011); *Yordanova v. Bulgaria*, Application no. 25446/06, (5 June 2012).

[63] Francesca Ippolito, "(De)Constructing Children's Vulnerability under European Law.", 23–27.

[64] Peroni and Timmer, "Vulnerable Groups," 1063–64.

[66] Ibidem, 1076–83.

[65] Chapman v. The United Kingdom, §96.

[67] M.S.S. v. Belgium and Greece, §249; Yordanova v. Bulgaria, §130.

[68] Yordanova v. Bulgaria, §130.

[69] Kiyutin v. Russia, 2011, §63.

neither the Charter of Fundamental Rights nor the Treaty of the European Union and the Treaty on the Functioning of the EU contains a single reference to vulnerable persons, special considerations of vulnerable individuals can be found in several pieces of EU legislation.

One of the first legal mentions of personal vulnerability was in 1983 Council Decision on the European Social Fund.[70] The preamble refers to "categories of persons who are particularly vulnerable on the labour market (in particular women, the handicapped and migrants)". The following year, two other Council acts referred to vulnerable persons, always in the field of the market (in particular disabled workers).[71] In 1990 the concept of vulnerability was then used in the even more context-dependent case of road users. It is the case of Council Directive on Civil Liability insurances,[72] whose preamble referred to *motor vehicle passengers* as "vulnerable category of potential victims". However, for many years vulnerable groups were mentioned only in the preambles of legal texts. For the first time, in 1994, the notion of vulnerability was included in one article of a European Directive: it is the case of young workers.[73]

Over the years, the notion of vulnerability slowly appeared in different socio-legal contexts to describe a variety of groups, as illustrated in Table 1. Examples of legal instruments that refer to vulnerability of particular groups range from employment, biomedical research, migration policy, to social assistance. Importantly, those instruments do not always describe those vulnerable groups in detail. Sometimes they even refer to the universal and inherent concept of vulnerability as in the first medical device directive ("the vulnerability of human body").[74]

Two fields of EU law, namely consumer protection law and the regulation on clinical trials, require some more attention, as they generated meaningful theoretical and practical discussions about the notion of vulnerability that could also be imported in the data protection discourse.

4.2.1. *Vulnerable consumers in the EU law*

The first explicit application of the notion of vulnerability in the consumer field can be found in the Directive 97/55/EC on misleading advertising.[75] Recital 22 allowed Member States to limit comparative advertising, in particular for advertising which targeted *vulnerable consumer groups*.[76] As we observe

Table 1 – Examples of vulnerable groups in EU law.

Field of law	Vulnerable groups
Employment	– "pregnant workers, workers who have recently given birth or who are breastfeeding"[77] "women, migrants and domestic workers, some undeclared workers"[78]
Biomedical research	– "prisoners and cognitively impaired patients"[79] – "frail or older people, people suffering from multiple chronic conditions, and people affected by mental health disorders"[80]
Public health	– "pregnant women and children"[81]
Migration	– "children and unaccompanied minors"[82]
Social assistance	– "persons with disabilities, refugees and displaced persons"[83]
Regulation of road traffic	– "blind, visually impaired and aurally challenged pedestrians, cyclists and children"[84]
Consumer rights	– "elderly and other vulnerable users"[85] – "vulnerable households, including those affected by energy poverty"[86]

[70] Council Decision of 17 October 1983 on the tasks of the European Social Fund, 83/516/EEC.

[71] Council resolution of 27 February 1984 on a second programme of action of the European Communities on safety and health at work, 84/C 67/02.

[72] Third Council Directive 90/232/EEC of 14 May 1990 on the approximation of the laws of the Member States relating to insurance against civil liability in respect of the use of motor vehicles.

[73] Council Directive 94/33/EC of 22 June 1994 on the protection of young people at work.

[74] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices.

[75] Directive 97/55/EC of European Parliament and of the Council of 6 October 1997 amending Directive 84/450/EEC concerning misleading advertising so as to include comparative advertising.

[76] Surprisingly, this directive has been repealed by "Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version)" that has no more reference to vulnerable persons.

[77] Council Directive 92/85/EEC of 19 October 1992 on the introduction of measures to encourage improvements in the safety and health at work of pregnant workers and workers who have recently given birth or are breastfeeding (tenth individual Directive within the meaning of Article 16 (1) of Directive 89/391/EEC).

[78] Directive 2014/54/EU of the European Parliament and of the Council of 16 April 2014 on measures facilitating the exercise of rights conferred on workers in the context of freedom of movement for workers, recital 5 refers to workers as vulnerable persons.

[79] Council Decision of 15 December 1994 adopting a specific programme of research and technological development, including demonstration, in the field of biomedicine and health (1994 to 1998), 94/913/EC, Annex I, § 7.

[80] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use.

[81] Decision No. 646/96/EC of the European Parliament and of the Council of 29 March 1996 adopting an action plan to combat cancer within the framework for action in the field of public health (1996 to 2000).

[82] Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted, now repealed by Directive 2011/95/EU, Article 20(3).

[83] Regulation (EU) No 231/2014 of the European Parliament and of the Council of 11 March 2014 establishing an Instrument for Pre-accession Assistance (IPA II).

[84] Regulation (EU) No 540/2014 of the European Parliament and of the Council of 16 April 2014 on the sound level of motor vehicles and of replacement silencing systems, and amending Directive 2007/46/EC and repealing Directive 70/157/EC.

[85] Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions.

[86] Directive (EU) 2018/2002 of the European Parliament and of the Council of 11 December 2018 amending Directive 2012/27/EU on energy efficiency.

in Table 1, consumer law took into account consumer vulnerability also in specific sectors, like energy or e-payments.

In more general terms, the Directive 2005/29/EC, the so-called Unfair Commercial Practice Directive (UCPD), refers in Article 5(3) to vulnerable groups of consumers as "people particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity". The recognition of those vulnerable consumers is based on the idea that they should be ensured a higher level of protection than 'the average consumer' referred to in Article 5(2).[87] However, the understanding of vulnerability in the UCPD is a matter of vivid discussion. For example, a report of the European Commission in 2016 confirmed the gradual nature of vulnerability,[88] in particular highlighting that the notion of vulnerable consumers should be assessed on several elements, "as a result of socio-demographic characteristics, behavioural characteristics, personal situation or market environment".[89] Additionally, the Study has also argued that consumer vulnerability is "multi-dimensional"[90] and so is "the impact of personal characteristics on the likelihood of being vulnerable as a consumer". For example, "characteristics like age and gender can increase vulnerability in some dimensions, but not in others".[91] The discussion about vulnerability in the UCPD also stresses the limitations about the division between "average" and "vulnerable" consumers and focus on temporal, gradual and contextual-relational aspects.[92] Interestingly, the European Commission has also recently relayed on the gradual approach to vulnerability in the Guidelines for the General Product Safety Directive.[93]

4.2.2. *Vulnerable research subjects in the EU law*

A second important legal field that generates a substantial discussion about human vulnerability is the regulation of biomedical research. At the EU level, the Clinical Trials Regulation (CTR) of 2014 is one of the most interesting pieces of legislation dealing with this topic.[94]

The CTR addresses the question of vulnerable research subjects under different perspectives. Article 10, whose title is "specific considerations for vulnerable populations", requires that for specific groups (minors, incapacitated subjects, pregnant or breastfeeding women, or 'other specific groups or subgroups') specific consideration shall be given to the assessment of the application for authorization[95] of a clinical trial. This provision does not clarify whether this "specific consideration" should be dedicated to the *decisional vulnerability* of such research subjects (i.e. their higher difficulty in giving consent to their involvement in the research)[96] or to the *higher risks of harms* that these subjects might encounter during a medical research project.[97]

Articles 31–33 address more specifically decisional vulnerability. These articles dictate particular rules for obtaining free consent from and giving adequate information to minors (Article 31), incapacitated subjects (Article 32), pregnant or breastfeeding women (Article 33). Member States can even guarantee further protection for other subjects in a situation of institutional or hierarchical dependency likely to influence their freedom of consent (Article 34).[98] In terms of decisional vulnerability, recital 31 mentions incidentally another category of vulnerable subjects that should require specific attention when collecting informed consent: individuals belonging to "an economically or socially disadvantaged group or in a situation of institutional or hierarchical dependency that could inappropriately influence her or his decision to participate".

A further reference to vulnerable people is at recital 15. Here the notion of vulnerability does not refer to decisional vulnerability, but to the weaker health conditions of specific categories of persons that the research should take into account. The reference to vulnerable groups at recital 15 aims to encourage specific medical research for vulnerable people, in order to avoid underrepresentation of vulnerable groups. In other words, this recital does not provide any particular safeguard or limitations for protecting vulnerable research

[87] European Commission, Staff Working Document Guidance on the implementation/application of directive 2005/29/EC on Unfair Commercial Practices accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses, SWD/2016/0163 final, § 2.6.

[88] European Commission, *Consumer vulnerability across key markets in the European Union*, Final report, January 2016, https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf.

[89] Ibidem.

[90] Stacey Menzel Baker, James W Gentry and Terri L Rittenburg, 'Building Understanding of the Domain of Consumer Vulnerability': [2005] Journal of Macromarketing 128, 134–135.

[91] Ibidem.

[92] European Parliament resolution of 22 May 2012 on a strategy for strengthening the rights of vulnerable consumers (2011/2272(INI)), § 1, Fred W. Morgan, Drue K. Schuler, and Jeffrey J. Stoltman, "A Framework for Examining the Legal Status of Vulnerable Consumers," *Journal of Public Policy & Marketing* 14, no. 2 (1995): 275.

[93] Commission Decision of 16 December 2009 laying down guidelines for the management of the Community Rapid Information System RAPEX established under Article 12 and of the notification procedure established under Article 11 of Directive 2001/95/EC (the General Product Safety Directive) (notified under document C(2009) 9843) Table 1.

[94] "Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on Clinical Trials on Medicinal Products for Human Use, and Repealing Directive 2001/20/EC Text with EEA Relevance," Pub. L. No. 32014R0536, 158 OJ L (2014).

[95] As regards authorization procedures that ethics committee should follow for clinical trials see in particular Chapter II (Articles 5–9) of the Clinical Trials Regulation.

[96] Council of Europe, Convention for the protection of human rights and the dignity of human beings with regard to the application of biology and medicine. Oviedo: 1997; ETS no. 164. Council of Europe. Additional Protocol to the Convention on Human Rights and Biomedicine, concerning biomedical research. Strasbourg 2005. CETS no. 195.

[97] Gennet, Andorno, and Elger, "Does the New EU Regulation on Clinical Trials Adequately Protect Vulnerable Research Participants?," 925–31.

[98] Namely: "persons performing mandatory military service, persons deprived of liberty, persons who, due to a judicial decision, cannot take part in clinical trials, or persons in residential care institutions".

subjects: on the contrary, it encourages to involve more vulnerable individuals in research projects.[99]

5. Beyond dichotomies: layers of vulnerability in the GDPR and the risk-based approach

After this overview, we can argue that in the EU, there is no single definition of vulnerable individuals. Although in several sectors we observed specific lists of vulnerable subjects, the general picture reveals a highly contextual and relational understanding of vulnerability based on power imbalance (as also the GDPR suggests). As regards the manifestation of vulnerability, although in the research field decisional vulnerability plays an important role, other legal fields present strong links between vulnerability and *harms*. Being vulnerable – across different legal sectors – generally means being more exposed to harms (if compared to other individuals) in some particular contexts.[100]

Connecting this analysis to the overview of vulnerability theories (Section 3), it seems to us that the EU legal approach to individual vulnerability can well fit with the layered-vulnerability idea proposed by Luna.[101] Her theory – based on layers of vulnerability (i.e. universal vulnerability tempered by an evaluation of different degrees of weakness) – can perhaps well describe the relational and contextual notion of vulnerability that we find in the EU law and in particular in the data protection field.

As we mentioned before, the notion of vulnerability is present and central to the data protection law and practice, although it is not adequately recognised yet. This results in limited capability of the data protection debate to acknowledge inequalities and contextually framed situations of different data subjects. We believe that implying vulnerability as one of the interpretative frameworks could address those limits and unleash the GDPR potential in responding to particularly harmful practices that affect those in a disadvantaged position. However, to do that, we need to overcome problematic dichotomies present in vulnerability theory. As we mentioned above, Luna's layered theory might offer some preliminary solutions. The theory of layered vulnerability[102] has had success in the academic debate[103] because it may solve both the limits of vulnerability as a label (source of stigmatisation) and the limits of universal vulnerability (if everyone is vulnerable, the notion will lose its usefulness in protecting weaker individuals). Layered understanding of vulnerability can also bring some certainty to the mitigation strategies and address some confusion between harm-based and procedural approaches. Luna in her recent article on layers of vulnerability tried to operationalise the concept and propose a method to identify and assess different layers of vulnerability. In particular, she recommends assessing risks of vulnerability considering two factors: *the harmfulness of effects* and the *likelihood* of risks.[104]

5.1. *The layered approach to vulnerability and the risk-based approach in the GDPR*

As noted by Gennet et al., Luna's theory adopts a risk-based definition of vulnerable persons. Interestingly, in the GDPR the notion of risks to fundamental rights and freedoms is pivotal. In particular, according to the risk-based approach in the GDPR (Article 24), the data controller is obliged to implement appropriate technical and organisational measures to ensure the compliance with the data protection principles: "taking into account the nature, scope, context and purposes of processing as well as the *risks of varying likelihood and severity* for the rights and freedoms of natural persons".[105] When assessing such risks of varying likelihood and severity for rights and freedoms, the controller should of course consider situations in which a certain data processing could damage more some particular (vulnerable) individuals.

Indeed, vulnerable persons are often defined as persons at higher risks (in terms of likelihood and severity) of damages to their rights and freedoms.[106] The notion of severity and likelihood seems perfectly in line with the two criteria for evaluating vulnerability layers in Luna's theory (harmfulness of effects and likelihood). Therefore, the risk-based approach can play a significant role in recognising and conceptualising the variety of risks (and layers) that can amplify, expose and exploit different vulnerabilities. Furthermore, it helps extend the scope of the GDPR to problems that are not traditionally related to the data protection discourse, like discrimination or inequality. This aspect of the risk-based approach plays, a significant role in mitigating potentially harmful outcomes of data-driven technologies.

Also, according to the principle of data protection by design (Article 25), the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles. Even in this case the controller should take into account "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons", but also "the state of the art [and] the cost of implementation".

The difference between Article 24 and Article 25 is that in the first case the data controller should merely prove his or her

[99] Gennet, Andorno, and Elger, "Does the New EU Regulation on Clinical Trials Adequately Protect Vulnerable Research Participants?," 929.

[100] Peroni and Timmer, "Vulnerable Groups," 1058 and 1064–67; Gennet, Andorno, and Elger, "Does the New EU Regulation on Clinical Trials Adequately Protect Vulnerable Research Participants?," 926.

[101] Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2 International Journal of Feminist Approaches to Bioethics 121; Florencia Luna, 'Identifying and Evaluating Layers of Vulnerability – a Way Forward' (2019) 19 Developing World Bioethics 86.

[102] See general: Luna, "Identifying and Evaluating Layers of Vulnerability – a Way Forward"; and "Elucidating the Concept of Vulnerability: Layers Not Labels".

[103] Gennet, Andorno, and Elger, "Does the New EU Regulation on Clinical Trials Adequately Protect Vulnerable Research Participants?," 926.

[104] Luna, "Elucidating the Concept of Vulnerability: Layers Not Labels," 89.

[105] Emphasis added.

[106] Luna, "Identifying and Evaluating Layers of Vulnerability – a Way Forward," 86–95.

compliance with the data protection principles. In the latter he or she should also "implement" data-protection principles (according to what is proportional to the state of the art and the costs of implementation).[107] In both cases, the attention to vulnerable data subjects and the implementation of specific safeguards to protect their rights and freedoms (i.e. to mitigate factors of vulnerability) seems necessary.

One further protection for vulnerable data subjects is the Data Protection Impact Assessment (DPIA). As already explained above, Article 35 (as interpreted by recital 75 and by WP29) requires performing a DPIA in case of high-risk data processing, including the case where the data subjects can be considered vulnerable. The DPIA is based on several steps (Article 35(7)): the systematic description of the processing, the assessment of necessity and proportionality, the assessment of risks and the description of measures envisaged to mitigate such risks. In other words, even according to the accountability principle, it is the controller who should autonomously determine measures for protecting vulnerable individuals.

It is clear that each measure should be linked to a risk. We have often referred to vulnerable subjects under different risk factors: in particular, decisional vulnerability and risks of more significant harms. Data controllers may suggest mitigation measures for particular vulnerable groups: e.g., in case of decisional vulnerability, the data controller could implement specific forms of consent or information disclosure measures; in case of individuals that might be easily discriminated, the data controller could implement periodical audits against discrimination, etc.

In addition, the DPIA can also overcome tensions between the notion of vulnerability as a risk *within* the processing and the notion of vulnerability as an *outcome* of the data processing. The holistic approach of Article 35 requires to analyse risks broadly, and also to systematically describe the data processing and assessing its necessity and proportionality.

We observe that such rules might appear as blank provisions, conditional to the will and activity of the data controller.[108] However, some tools could reduce arbitrariness of data controllers: e.g., codes of conduct could better specify what to do in case of vulnerable data subjects, in specific sectors ;[109] certification mechanism could also help.[110] Also, the Data Protection Authorities (DPAs) (e.g. through their powers, according to – inter alia – Article 36 about prior notifications) could release clear guidelines on how to deal with some vulnerable individuals.[111]

5.2. *Legal bases for processing data of vulnerable subjects*

The layered-based notion of vulnerability and the risk-based approach can be a key also for addressing the issue of decisional vulnerability: is consent an adequate legal basis for vulnerable individuals? If yes, should consent be accompanied by more tailored information? If not, are there better legal bases for processing vulnerable persons' data or the data controller should avoid processing those data?

According to Article 24, the data controller needs to analyse the level of risk (for fundamental rights and freedoms of data subjects) and so the level of vulnerability of the data subject before proceeding with the data processing. Accordingly, when choosing the legal basis for data processing (consent, legitimate interests), it is necessary to do a vulnerability layers-evaluation of the data subjects and adapt the safeguards.

As mentioned above, the only vulnerable category that has group-specific protection under the GDPR is the category of children. Their specific protection is mostly based on two elements: consent and information duties of data controllers. When data processing is based on consent and relates to the offer of information society services, under a certain age (16 years, that Member States can reduce to 13) consent should be given or authorised by the holder of parental responsibility for the child (Article 8). At the same time, transparency duties and any communication within the exercise of data protection rights, should be "in a concise transparent, intelligible and easily accessible form, using clear and plain language, *in particular for any information addressed specifically to a child*"[112] (Article 12(1)).

One might wonder whether, by analogy, these safeguards could also be used for other (adult) vulnerable data subjects. Interestingly, the WP29 guidelines on consent, when referring to the child's consent in Article 8, affirm: "[c]ompared to the current directive, the GDPR creates an additional layer of protection *where personal data of vulnerable natural persons, especially children, are processed*".[113] This sentence seems to suggest that special rules for consent were conceived for all vulnerable natural persons: "especially children" does not mean "only children". However, parental consent for information society services is a special rule that cannot be easily applied in different contexts. The only similarity with some "vulnerable adults" is that legally incapacitated persons might need consent (or authorisation to consent) from their legal representatives, according to the national laws.[114] In more general terms, we could assume that data controllers should adopt special safeguards when collecting consent from *vulnerable adults*.

This is in line with the characteristics of consent under Articles 4(11) and 7: freely given, specific, informed and unambiguous. Consent is free only if the data subject is capable of choosing whether to give consent and controlling how to give and withdraw it.[115] In particular, WP29 adds: "any element of inappropriate pressure or influence upon the data subject

[107] Lina Jasmontaite and others, 'Data Protection by Design and by Default': (2018) 4 European Data Protection Law Review 168.

[108] See, e.g., Ann Cavoukian, Alexander Dix and Khaled El Emam, 'The Unintended Consequences of Privacy Paternalism' (Information and Privacy Commissioner, Ontario, Canada), 7–8 <https://collections.ola.org/mon/28003/326077.pdf>.

[109] See Articles 40–41 of the GDPR.

[110] See Article 42 of the GDPR.

[111] See Section 5.f.

[112] Emphasis added.

[113] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, WP 259 rev.01, 23. Emphasis added.

[114] Article 8(3) GDPR clarifies that special rules for child's consent "shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child".

[115] Article 29 Working Party, Guidelines on Consent, 5: "The element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure nega-

(which may be manifested in many different ways) which prevents a data subject from exercising [her] free will, shall render the consent invalid".[116] In other words, when the data subject is in a situation of decisional vulnerability, consent should not be valid.

Recital 43 relates the idea of freedom of consent to the notion of power imbalance: "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case *where there is a clear imbalance between the data subject and the controller*, in particular where the controller is a public authority". We already observed how individual vulnerability is defined, especially in the data protection field, as power imbalance between controllers and subjects.[117] WP29 explains that imbalances of power are not limited to public authorities but also include the relationship between employees and employers and even other situations: "[c]onsent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will".[118] In other words, consent should not be a legal basis when the data subject can be in a situation of *decisional* vulnerability. The EDPB Opinion on Clinical Trials Regulation also highlights that consent should not be a legal basis for data processing in case of vulnerable data subjects. In particular when the potential subject is not "in good health conditions" or "belongs to an economically or socially disadvantaged group, or is in a situation of institutional or hierarchical dependency that could inappropriately influence her or his decision to participate".[119]

However, we remark that consent should be avoided not in all cases of vulnerable data subjects, but only when the data subjects are affected by decisional vulnerability.[120] In other cases, consent is not only possible but even recommended: this is why WP29 Guidelines on Purpose Limitation affirm that further processing of data (the so-called repurposing of data processing) for vulnerable data subjects should be possible just upon consent.[121] In that context, the notion of vulnerable individuals seems associated with the risk of, e.g., discrimination, rather than to situations of decisional vulnerability.[122]

However, in a few cases, the decisional vulnerability can be mitigated with the adoption of better safeguards, in particular transparency safeguards. As we observed, Article 12 seems to require a very high standard of legibility for information policies and for other communications within the exercise of data protection rights.[123] If such communication is addressed to persons with reduced understanding (including – but not limited to – children), data controllers might be required to give information in a way that might be easily understandable by every recipient. Also, WP29 Guidelines on Transparency refer to other vulnerable positions: "if a data controller is aware that their goods/services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects".[124]

5.3. *Participation of vulnerable data subjects in the decision-making about data processing*

The layered approach to data subjects' vulnerability also requires mitigation strategies that are adequate to the particular context and situations. We explore some of the possible directions toward interpreting existing mechanism within the GDPR that could adequately react to vulnerability of certain groups. Those ideas include, for example, procedural safeguards related to participation or institutional responses.

Some authors have suggested involving individuals in the decision-making about research.[125] The participatory principle is also part of a long discussion within the human-computer interaction field in the context of designing technologies.[126]

If the participatory process is meaningful it can highlight and respond to experiences and situation of vulnerable com-

tive consequences if they do not consent, then consent will not be valid".

[116] Article 29 Working Party, Guidelines on Consent, 6.

[117] Article 29 Working Party, Guidelines on DPIA, 10: "Vulnerable data subjects may include […] any case where an imbalance in the relationship between the position of the data subject and the controller can be identified".

[118] Article 29 Working Party, Guidelines on Consent, 7.

[119] European Data Protection Board, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (art.70.1.b), 6,

[120] About the distinction between decisional vulnerability and other forms of vulnerability see Section 5(a).

[121] Article 29 Working Party, Opinion 03/2013 on purpose limitation, 32.

[122] Ibidem, 32: "further processing of personal data concerning health, data about children, other vulnerable individuals, or other highly sensitive information should, in principle, be permitted only with the consent of the data subject".

[123] About the notion of legibility see Richard Mortier et al., "Human-Data Interaction: The Human Face of the Data-Driven Society," *ArXiv:1412.6159 [Cs]*, October 6, 2014, http://arxiv.org/abs/1412.6159; Gianclaudio Malgieri and Giovanni Comandé, "Sensitive-by-Distance: Quasi-Health Data in the Algorithmic Era," *Information & Communications Technology Law* 26, no. 3 (2017): 229–49, https://doi.org/10.1080/13600834.2017.1335468; Gianclaudio Malgieri and Giovanni Comandé, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation," *International Data Privacy Law* 7, no. 4 (2017): 243–65, https://doi.org/10.1093/idpl/ipx019.

[124] Article 29 Working Party, Guidelines on Transparency, 9.

[125] See, e.g., Convention on the Elimination of All Forms of Discrimination against Women, *General Recommendation 30*, para. 57. See also: Veronika Flegar and Emma Iedema, "The Use of the 'Vulnerability' Label by the Committee on the Elimination of Discrimination Against Women: Protecting or Stigmatizing Women and Girls in the Forced Migration Context?", *Brill Open Law*, (2019): 27, https://doi.org/10.1163/23527072-20191021.

[126] Sasha Costanza-Chock, "Design Justice: Towards an Intersectional Feminist Framework for Design Theory and Practice" (Design Research Society Conference, Limerick, 2018), 10, https://doi.org/10.21606/drs.2018.679.

munities.[127] In the context of Big Data research, Jackson et al. argue that the engagement of vulnerable groups in research as participants but also contributors to study design, implementation, and the analysis can help address problem of discriminatory biases.[128] However participation in research and decision-making about data-driven technologies should also fulfil certain conditions. One example of such participatory-driven design process is the "Design Justice" project.[129] It recommends engaging with the questions about power, distribution of risks and benefits, reproduction of domination and oppression as well as creating a space for the more equitable and fair design process. The data protection field can use those insights to understand the role of participatory process in decision-making about data-driven technologies and their impact on fundamental rights.

Interestingly, the DPIA under the GDPR already provides some forms of participation of the data subjects. In particular, Article 35(9) states as follows: "where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations". Although the involvement of data subjects is required only when "appropriate",[130] the DPIA Guidelines envision that this input could be, for example, in the form of surveys crafted by data controllers and sent to future customers. Also, those Guidelines explain that if data controllers do not seek these external views, they must justify such decision.[131] In addition, if data controllers do seek these views and then disregard them, they must document why they have chosen to disregard external inputs.[132]

5.4. *Data protection as backstop for high-risk data processing*

In some cases, the vulnerable condition of the data subjects is so relevant that the data controllers could find no adequate safeguards to mitigate them: in these situations, the only way is not to start (or not to continue) the data processing.[133] Several scholars have indeed recently suggested that what is necessary is not only to mitigate risks of certain data processing but to avoid some kinds of data processing from the outset. For example, discussing AI systems and their possible discriminatory outcomes, Powles argues that instead of solving the problem of biases we need to wonder if particularly harmful data-driven systems should be used in the first place.[134]

In general terms, the mere application of the data protection principles at Article 5 could lead to avoiding certain data processing. In particular, the principle of fairness (Article 5(1), point a),[135] could serve as a barrier against data processing exploiting vulnerable data subjects.[136] Several authors have suggested that its goal is to mitigate excessive unfair imbalances between controllers and data subjects on a case-by-case basis. The natural consequence of such principle is that the data controller should avoid exploiting data subjects' factors of vulnerability.[137] In some cases, this may not be possible just through the implementation of suitable safeguards as required at Articles 24, 25 and 35: there might be no safeguards to rebalance the asymmetry between data controllers and vulnerable data subjects.[138]

Another principle that could act as a backstop against the exploitation of vulnerable data subject is the principle of lawfulness (Article 5(1), point a): in some cases, there might be no adequate legal bases to process data of vulnerable data subjects. We already observed above that consent is not always an adequate legal basis, in particular in case of decisional vulnerability of data subjects. In those cases, the data controller

[127] Haiyi Zhu et al., "Value-Sensitive Algorithm Design: Method, Case Study, and Lessons", *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (2018): 1–23, https://doi.org/10.1145/3274463.

[128] Latifa Jackson et al., "Including Vulnerable Populations in the Assessment of Data From Vulnerable Populations," *Frontiers in Big Data* 2 (June 28, 2019): 7, https://doi.org/10.3389/fdata.2019.00019.

[129] Costanza-Chock, " Design Justice," 2.

[130] In the original proposal of the Commission, consultation with data subjects was mandatory (Article 33[4]). The Parliament's text argued that this 'represents a disproportionate burden on data controllers' (amendment 262). Accordingly, the approved Article 35(9) requires consultation only 'where appropriate' and 'without prejudice to the protection of commercial or public interests or the security of the processing operations''. See also: Reuben Binns, "Data Protection Impact Assessments: A Meta-Regulatory Approach", *International Data Privacy Law* 7, no. 1 (2017): 28, https://doi.org/10.1093/idpl/ipw027.

[131] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA), 15.

[132] Ibidem, 15.

[133] See, e.g., European Data Protection Board, Letter in reply to Sophie In't Veld, Ref: OUT2020-0004, 29 January 2020, 4.

[134] Julia Powles, "The Seductive Diversion of 'Solving' Bias in Artificial Intelligence," 2018, https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53.

[135] Similarly, also the principle of legitimacy of purposes (Article 5(1) point b) could serve as a barrier against the exploitation of vulnerable data subjects.

[136] See the centrality of the notion of fairness in the vulnerability discourse: Florencia Luna, "Elucidating the Concept of Vulnerability: Layers Not Labels," *International Journal of Feminist Approaches to Bioethics* 2, no. 1 (2009): 126.

[137] Damian Clifford and Jef Ausloos, "Data Protection and the Role of Fairness", *Yearbook of European Law* 37 (2018): 130, https://doi.org/10.1093/yel/yey004; Inge Graef, Damian Clifford and Peggy Valcke, "Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law," *International Data Privacy Law* 8 (2018): 200, https://doi.org/10.1093/idpl/ipy013; Michael Butterworth, "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework," *Computer Law & Security Review* 34 (2018): 257, https://doi.org/10.1016/j.clsr.2018.01.004; Gianclaudio Malgieri, "The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation", *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2020), https://doi.org/10.1145/3351095.3372868.

[138] This might be the case of researches, whose research goal is explicitly based on the exploitation of vulnerable situations (e.g. understanding sexual orientation of people in specific countries where homosexuality is criminalized, etc.). Or cases where any safeguards might be useless: see Luna, 2019, 94, making the example of fertile women in countries where abortion is illegal who will not be able to adhere to and use birth control measures owing to their partners' refusal or because it may lead to intra-family violence, etc.

should choose another legal basis under article 6.[139] If it is not possible to process data on the basis of contract, legal obligation, public interest and vital interests, the data controller might consider processing data on the basis of legitimate interest (Article 6(1) point f). However, even in that case, she is asked to assess the balancing between her interests and the data subject's ones. In such assessment, WP29 suggests considering, inter alia, "the status of the data controller and data subject, including the balance of power between the data subject and the data controller, or whether the data subject is a child or otherwise belongs to a more vulnerable segment of the population. (…) It is important to assess the effect of actual processing on particular individuals".[140] In other words, it might be the case that considering the particular effects of a data processing, the right to privacy and data protection of vulnerable data subjects prevails on the legitimate interest of the data controller: in this case the data processing should not start at all.

In addition, Article 36 (as interpreted through recital 94) describes when data controller needs to consult the DPA before the processing activities. Such prior consultation is necessary if the DPIA reveals that the processing would result (in the absence of safeguards, security measures and mechanisms to mitigate the risk) in high risks to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation.

Interestingly, recital 94 explains that these cases of high risks are "likely to result from certain types of processing and the extent and frequency of processing, which may also result in a realization of damage or interference with the rights and freedoms of the natural person". In other words, there might be cases of higher risks of damages (i.e. cases of *vulnerable* individuals as explained above) that cannot be mitigated through particular measures.

Once consulted, the DPA could give specific indications about safeguards to adopt in the particular situations, but may also "use any of its powers referred to in Article 58" (Article 36(2)), including the power to impose a temporary or definitive limitation including a ban on processing (Article 58(2), point f). In other words, if the risk assessment (the "vulnerability layers" assessment) reveals high risks that could not be mitigated through reasonable efforts, a system of cooperative governance between controllers and DPAs could take place. However the DPAs could even prohibit certain data processing where specific forms of vulnerability of certain data subjects cannot be rebalanced.

5.5. *Data protection agencies as a responsive authority*

The notion of vulnerability can also play a role in the operations of DPAs.[141] Theoreticians in the vulnerability field call for institutional responses to certain dependencies, inequalities or capabilities of specific groups.[142] Such a way of looking at DPAs is mentioned just once in the GDPR. Under Article 57, DPAs should conduct specific activities, including raising public awareness about data protection (point b). When carrying out this task, DPAs should pay special attention to addressing the situation of children. This approach is consistent with other provisions that construct a special position of children in the GDPR. Indeed, some national DPAs already took actions toward promoting knowledge about data protection in schools or try to come with particular guidelines addressing the situation of children.[143]

However, the question remains if and how vulnerability can act as a paradigm in conducting other activities, especially those that have a substantial aspect like handling complaints, carrying inspections or imposing fines. Another aspect to consider is the risk limitations of access to authorities and obstacles in receiving redress when data rights are violated. As the Fundamental Rights Agency emphasised, individuals belonging to vulnerable groups may face structural problems, like lack of financial resources, inadequate level of legal literacy and empowerment in exercising access to justice in general.[144] Similar problems can be experienced in the data protection field.[145] That is why there might be a particular responsibility of DPAs (and broader national legal systems) to ensure that they take necessary steps to grant people belonging to such vulnerable groups access to redress mechanisms.

As it was already mentioned, DPAs may also use their powers under the mechanism of a priori consultation, when processing of personal data would result in a high risk to the fundamental rights and freedoms (Article 36 and 58(3), point a). In such a situation, DPAs may issue recommendations and guidelines if the processing is related to vulnerable individuals. DPAs' power related to guidance, consultation, and opinions can be enforced vis-à-vis national legislations

[139] About the limits of consent see in general Gabriella Fortuna-Zanfir, "Forgetting about Consent. Why the Focus Should Be on 'Suitable Safeguards' in Data Protection Law," in *Reloading Data Protection*, ed. Serge Gutwirth, Ronald Leenes, Paul De Hert (Springer, 2014), 237–55; Bart W. Schermer, Bart Custers, and Simone van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection," *Ethics and Information Technology* 16, no. 2 (2014): 171–82, https://doi.org/10.1007/s10676-014-9343-8; Bart Custers et al., "Consent and Privacy," in *The Routledge Handbook of the Ethics of Consent*, ed. Andreas Müller and Peter Schaber (London: Routledge, 2019).

[140] Article 29 Working Party, Opinion on purpose limitation, 51.

[141] About the idea of cooperation between single data controllers (that need to implement the accountability principle) and public supervisory entities see Margot E. Kaminski, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability," *Southern California Law Review* 92, no. 6 (2019), https://papers.ssrn.com/abstract=3351404.

[142] Fineman, "The Vulnerable Subject," 8–10.

[143] For example: Agencia Española de Protección de Datos, „Memoria 2016", 2107, https://www.aepd.es/media/memorias/memoria-AEPD-2016.pdf; Information Commissioner's Offices, "Age appropriate design: a code of practice for online services", 2016 https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services/

[144] Fundamental Rights Agency, Handbook on European Law Relating to Access to Justice (Luxembourg: Publications Office of the European Union, 2016).

[145] Fundamental Rights Agency, "Access to Data Protection Remedies in the EU Member States" (Luxembourg: Publications Office of the European Union, 2013).

and code of conducts (see Article 58). In all those instances, DPAs may take into account situations of vulnerable individuals and specify how processing of personal data could be performed.

6. Concluding thoughts

The vulnerability-aware interpretation of data protection law may provide a meaningful response to many shortcomings of the existing discourse and practices around the data protection rights. Firstly, contrarily to other fields, like consumer protection, the data protection discourse has never really developed the notion of the data subject and the possible layers of data subjects in terms of awareness, understanding and weakness (e.g., the "average data subject" versus the "vulnerable data subjects). Secondly, privacy and data protection have a potential to be understood as a framework that allows rebalancing situations of individual vulnerability (see, in particular, Calo's theory of privacy and vulnerability).[146] Thirdly, the rise of data-driven technologies that may serve as tools for exploitation, manipulation, and discrimination of marginalised communities and individuals in particular life situations require a robust and effective use of existing legal instruments that could mitigate individual and collective harms.

Here we propose to focus on the important role for the notion of vulnerability as a principle that is coherent with the data protection values and legal constructions. Indeed, vulnerability can be seen as one of the driving forces in data protection, which is related to the recognition of inferiority, dependency, and subjugation of individuals in the context of processing data. Although this relation was rarely stressed and explained explicitly. We also believe that vulnerability can help identify and address situations of individuals and groups, which require specific protection.[147] The recognition of the particular vulnerability of some data subjects can be translated into tailored safeguards or institutional interventions that take into account the vulnerable position of data subjects. This is also a way to introduce some additional "duties of cares" to the operation of data controllers and DPAs.[148] It can also have important implications for addressing problems of automated discrimination and manipulation. Seen through the lenses of vulnerability, responses to algorithmically mediated discrimination or manipulation move beyond the narrow interventions that focus on transparency or explainability and try to offer a more holistic approach that use the whole system of the GDPR in understanding, minimising and mitigating potentially harmful positions of data subjects.

However, the data subjects' vulnerability is involved in problematic dichotomies (universalistic versus particular approach and vulnerability within the data processing versus vulnerability related to the outcome of the data processing). To overcome some of the problems that emerge from these dichotomies, we turn to Luna's theory of layered vulnerability. We believe it might present the most suitable approach to the complex relation between data-driven technologies and fundamental rights (and, in particular, the right to data protection). Our vulnerability-aware interpretation follows this theory and argues for using the open clauses in the GDPR to provide adequate protection to vulnerable data subjects. Indeed, the notion of risks for fundamental rights in the GDPR is in line with the idea of vulnerability as higher risks of harms for some individuals. Accordingly, the data protection by design and the DPIA could be tools to implement specific safeguards for vulnerable individuals. Other data protection principles and rules (the concept of fairness, transparency duties, the concept of lawfulness and the role of consent, the role of DPAs and the broader participation of data-subjects in decision making about data processing) can also play a similarly important role in framing the protection of vulnerable data subjects.

Altogether we see vulnerability as a powerful interpretative and narrative tool that could bring responsiveness and duty of care to the data protection field. However, further reflection and conceptualisation is still required. Many of the problems described in this article have been only hinted, and we hope to explore them in further works, in particular the relationship between the layered conception of vulnerability and risk assessment, the impact of different manifestations vulnerabilities in exercising data protection rights and the role of DPAs.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

[146] Calo,"Privacy, Vulnerability, and Affordance", 15.

[147] Similar argument in bioethics field in Wendy Rogers, Catriona Mackenzie, and Susan Dodds, "Why Bioethics Needs a Concept of Vulnerability," 11–38.

[148] Peter Blume, "The Data Subject," 259; Jack M. Balkin, "Fixing Social Media's Grand Bargain," *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1814* (2018): 12, https://www.hoover.org/sites/default/files/research/docs/balkin_webreadypdf.pdf.