EJLT European Journal of Law and Technology

The vulnerable data subject: A gendered data subject?

Gianclaudio Malgieri* **Gloria González Fuster****

Abstract

Vulnerability is an emerging topic in many different fields, but data protection and privacy discussions of vulnerability have rarely engaged with gender studies. This paper investigates the notion of the 'vulnerable data subject' from a gender perspective, to question whether gender should be regarded as factor of vulnerability at all, and, if yes, how. It also asks what do these reflections tell us about the (gendered or un-gendered) notion of 'standard data subject'. Even though the term 'vulnerable data subject' is only incidentally mentioned in EU data protection law, and in the GDPR only referring explicitly to children, several Data Protection Authorities (e.g. in Spain and Poland) have considered "being female" as a potential source of data subject's vulnerability (e.g. in case of consumers victims of sex-related crimes). The US privacy tort – as originally conceived – was built off gendered notions of female modesty, suggesting women were vulnerable, and connecting women's privacy claims to the 'wrong kind of privacy'. Looking at the history and foundations of privacy and data protection law, surface questions such as whether the 'average data subject' in privacy and data protection legislation is, by default, a man, and whether women might have to be regarded as vulnerable data subjects just because they are women. This article then looks into law and economics analysis of consumers' behaviour, but also political philosophy and, in particular, gender studies, to observe an intellectual polarisation: on the one hand the universalist approach, according to which every human must be regarded as vulnerable, as otherwise vulnerability would be a stigmatising label; on the other hand the particularistic approach, according to which some subjects are more vulnerable than others (in particular, women are more vulnerable – i.e. subject to adverse effects – than men in many contexts: workplace, education, etc.). A third way might be the 'layered' theory of Luna, based on a contextual and relational (even situational) nature of vulnerability. This solution is compatible with the layered risk-based approach in the GDPR, but also with intersectional approaches in gender studies. This 'third way' might be also a cautious solution to the ambiguous and inconsistent

* Prof Dr Gianclaudio Malgieri, Associate Professor of Law, EDHC Business School.

** Prof Dr Gloria Gonzalez Fuster, Research Professor, Vrije Universiteit Brussel (VUB).

treatment of vulnerability both in the European Union policies surrounding data protection law and in the EU data protection practice itself (considering, e.g. the ineffective protection of children).

1. Introduction: gender, vulnerability and data protection

Vulnerability is an emerging topic in many different fields, and it is increasingly important in data protection and privacy law. Whereas academic and policy discussions about technological developments such as Artificial Intelligence (AI) almost systematically highlight the different impact of these developments on individuals depending on their gender, European data protection law remains – at least on the surface – generally unconcerned with gender. Specifically, the discussions around vulnerability in data protection law have rarely engaged with gender studies, or feminist perspectives.[1]

This paper investigates the notion of the 'vulnerable data subject' from a gender perspective to question whether gender is and/or should be regarded as a factor of vulnerability at all for the purposes of data protection, and, if yes, how. This investigation into the notion of the vulnerable data subject is intrinsically connected with a reflection on the 'standard data subject',[2] to the extent that the construction of the notion of this vulnerable data subject as gendered might be revealing of a prior gendering of the standard, normal, 'mere' data subject.

Two preliminary disclaimers are necessary. First, the notion of vulnerable data subjects (and of vulnerable individuals in general) is not clear in the doctrine, and this paper does not pretend to cover this definitional gap once and for all. However, building on the normative elements scattered in EU (and extra-EU) law, the paper will delineate some of the characteristics that are common to vulnerable subjects in different contexts. Second, the dualism average/vulnerable subjects should not be perceived as black and white dichotomy. The vulnerable individual is not necessarily the opposite of the average individual, even if generally speaking the idea of average is construed as not-particularly-vulnerable. There are other conceptual antonyms for the vulnerable, such as 'the powerful' (the counterpart of the vulnerable subjects, e.g. the data controller that can exploit the data subjects' weaknesses) or 'the resilient' (similar data subjects that in the same contexts are not exposed to risks as much as vulnerable people). In addition, between the average and the vulnerable there is a whole range of intermediate layers of less or non-average and less or non-vulnerable people. The notions of average and vulnerable are dynamic,

[1] Data protection law as such has also until recently only exceptionally engaged with these perspectives; see, in this sense: Jens T. Theilen, Andrea Baur, Felix Bieker, Regina Ammicht Quinn, Marit Hansen and Gloria González Fuster, (2021), 'Feminist data protection: an introduction' Internet Policy Review, 10(4).

[2] Gianclaudio Malgieri and Jedrzej Niklas, 'The Vulnerable Data Subject' (2020) 37 Computer Law & Security Review.

and they are used here as the two conceptual poles of a spectrum of different subjective situations.

We enter this exploration aware of the fact that some scholars, in light of the many challenges encountered for the effective protection of individuals, and especially of vulnerable individuals, have suggested that a better path for individual protection against contemporary data practices might be not a refinement of the legal apprehension of people as 'data subjects' but rather a shift towards other types of protection – such as, for instance, not individual-focused but group-based 'group privacy'.[3] We also enter these reflections by acknowledging that viewpoints on the relations between privacy, data protection and gender are multiple and sometimes contrasted. In this sense, it has been highlighted that the United States (US) privacy tort – as originally conceived – was built off gendered notions of female modesty, suggesting women were vulnerable, '*seduced wives and daughters*'[4] in need of (male) help, and thus connecting women's privacy claims to a 'wrong kind of privacy'.[5] At the same time, also in a US context, the historical contribution of women to the emergence of modern privacy has also been documented,[6] and it would be difficult to even summarise the many ways in which the right to privacy has advanced women's rights.[7]

1.1 The notion of human vulnerability: looking for a definition

Some early definitions and conceptualisations of human vulnerability stressed its links to fragilities, harms and the fact of being wounded, as the word's etymology suggests ('vulnus' in Latin means wound).[8] The term served almost as a synonym for dependency,

---

[3] Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) <https://www.springer.com/gp/book/9783319466064> accessed 28 May 2021. Noting that 'group data protection' was already 'an essential part of any data protection regime in a Western democracy' in 1975: Frits W. Hondius, *Emerging Data Protection in Europe*, North-Holland Publishing Co, 1975, p. 99 (referring to Steinmüller).

[4] Anita Allen and Erin Mack, 'How Privacy Got Its Gender' [1991] Faculty Scholarship at Penn Law <https://scholarship.law.upenn.edu/faculty_scholarship/1309>.

[5] Scott Skinner-Thompson, 'Privacy's Double Standards' (2018) 93 Washington Law Review 2051.

[6] Jessica Lake, *The Face That Launched a Thousand Lawsuits: The American Women Who Forged a Right to Privacy* (Yale University Press 2016) <https://www.jstor.org/stable/j.ctt1gxxpmt> accessed 29 May 2021.

[7] Ranging from abortion cases to the right not to be subject to a strip search in case of traffic violation, just to give some examples (cf. for instance, Caroline Kennedy and Ellen Alderman, *The Right to Privacy* [1st edition, Alfred A Knopf 1995] 13.

[8] Catriona Mackenzie, Wendy Rogers and Susan Dodds, 'Introduction: what is vulnerability, and why does it matter for moral theory?', *Vulnerability* (Oxford University Press 2013) 4–5 <https://www.oxfordscholarship.com/10.1093/acprof:oso/9780199316649.001.0001/acprof-9780199316649-chapter-1>.

helplessness, pain, violence, and weakness. Goodin affirmed that 'to be vulnerable is to be susceptible to harm to one's interests'.[9]

A more mature and complex definition of human vulnerability can be found in the Council for International Organizations of Medical Science (CIOMS)'s notes on vulnerability. The notes refer to vulnerability not only as a susceptibility to harms, but also as the substantial incapability of protecting one's own interests.[10] Building on this definition, Schoreder and Gefenas tried to substantiate and delineate better vulnerability's key components: harm, interests, likelihood and protection capabilities.[11] Accordingly, they proposed the following definition: 'to be vulnerable means to face a significant probability of incurring an identifiable harm while substantially lacking ability and/or means to protect oneself'.[12] Many other scholars and institutions have followed this view of conceptualising vulnerability around the exposure and the likelihood of being harmed in the context of autonomy, dignity or integrity.[13]

However, vulnerability is a condition situated in opposition to an actual harm or injustice rather than indicating its potentiality.[14] Well-established views also stress that vulnerability is a condition that should be avoided, something negative and a risk that should be mitigated.[15] This latter approach was subject to some criticisms mostly from feminist scholars, who explored the positive sides of vulnerability, showing it as a precondition of empathy, social-connectedness and intimacy.[16] Therefore, vulnerability is not only a limitation but also something that allows us to act and feel, e.g. Erinn Gilson formulates vulnerability as 'openness to being affected and affecting'.[17]

Originally, vulnerability was analysed as 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, children, and people with

---

[9] Robert E Goodin, *Protecting the Vulnerable: A Reanalysis of Our Social Responsibilities* (University of Chicago Press 1985); See, similarly, also the vulnerability definition in Doris Schroeder and Eugenijus Gefenas, 'Vulnerability: Too Vague and Too Broad?' (2009) 18 Cambridge quarterly of healthcare ethics: CQ: the international journal of healthcare ethics committees 113.

[10] Council for International Organizations of Medical Science, 'International Ethical Guidelines for Biomedical Research Involving Human Subjects' (2002) <http://www.cioms.ch/frame_guidelines_nov_2002.htm>.

[11] Doris Schroeder and Eugenijus Gefenas, 'Vulnerability: Too Vague and Too Broad?' (2009) 18 Cambridge Quarterly of Healthcare Ethics 113.

[12] ibid., 117.

[13] Mackenzie, Rogers and Dodds (n 7) 6–11.

[14] Erinn C Gilson, *The Ethics of Vulnerability: A Feminist Analysis of Social Life and Practice* (2016) 7–8.

[15] Malgieri and Niklas (n 1).

[16] Alyson Cole, 'All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique' (2016) 17 Critical Horizons 260, 264.

[17] Gilson (n 13) 76.

[18] Martha Albertson Fineman, 'Beyond Identities: The Limits of an Antidiscrimination Approach to Equality' (2012) 92 Boston University Law Review, 59, 1750.

disabilities. This reflects a predominant way of using the concept of vulnerability in more practical circumstances like research, social policy, or policing.[19]

Commentators in the research ethics field have stressed that there are two ways of conceptualising and addressing the consequences of vulnerability.[20] The first approach focuses on the harms and the ways to eliminate them.[21] The second approach focuses on individuals' ability to overcome their vulnerable position and empower them with various decisional and procedural safeguards. In other terms, in the first approach, the emphasis is put on harm (physical or psychological); in the second, on consent or participation in decision-making.

1.2 Vulnerability insights from gender studies: the problems of labels

Several authors have criticised this way of understanding vulnerability, since it might bring stigmatising effects and harmful regulation for minorities.[22] Some critical scholars thus advocate reformulating the understanding of vulnerability as a *universal* human condition manifesting itself differently in different situations, periods and spaces. This concept is portrayed as a general feature of human existence, a characteristic of every human being.[23] For some, however, this emphasis on the universal character of vulnerability ignores structural violence, injustice and the exploitation experienced by particular groups.[24] Apologists of a universalised notion of vulnerability argue it can be a way to run away from failures of existing diversity and equality policies and anti-discrimination laws.[25]

---

[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] 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.

[21] 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.

[22] Cole (n 15) 262.

[23] 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.

[24] 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,

[25] Fineman (n 22) 18, 23 Another area of disputes about vulnerability concerns the organisational, legal and political responses to vulnerability. Fineman calls for responsive institutions that recognise human vulnerability. She criticises existing systems of rights and laws that depend on the formal equality and embrace an individualistic, self-sufficient and rationalist liberal subject. In a similar tone Goodin, vulnerability implies a justification for welfare state institutions that could help in addressing the lack of essential goods and services Goodin (n 8) 145.

A theory that attempts to overcome the universalism/particularism dichotomy of human vulnerability is the theory of layered vulnerability of Florencia Luna.[26] According to this theory, there exists layers of vulnerability, which are not static attributes of certain groups of individuals, but features constructed by status, time and location. The identification and assessment of vulnerability layers should be based on several criteria, including 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).

In line with this thinking, potentially any data subject could be, in a particular context or circumstance, vulnerable (e.g. due to the impossibility to provide free consent, or because they are subject to manipulation, discrimination, physical damages, etc.). Therefore, the analysis of vulnerability must focus on the *layered* relationship between the data controller and the data subject.[27] In other terms, what qualifies vulnerability is the specific power imbalance between data subjects and controllers considering all specific characteristics and the higher risk of adverse effects for individuals.

1.3 Privacy, data protection and gender(ed vulnerability)

Privacy has been both celebrated and decried by feminists, inviting a distinction between a '*distorted notion of privacy*', historically instrumental for the oppression of women, trans and gender diverse people, and other types of privacy, crucial precisely for the same individuals.[28] Much of the feminist critique of privacy has evolved around the public/private distinction, itself a major concern of feminist legal theorising.[29] Many of the arguments in this field have tried to counter the (mis)use of privacy to protect the perpetrators of domestic violence[30] or online abuses.[31] Contrasting and sometimes conflicting notions of privacy continue to coexist around the world, and they have for

[26] 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.
[27] See, extensively, Malgieri and Niklas (n 1).
[28] Privacy International, 'Report: From Oppression to Liberation: Reclaiming the Right to Privacy' (2019) <http://privacyinternational.org/report/2457/report-oppression-liberation-reclaiming-right-privacy> accessed 29 May 2021; The paradoxes of the uneasy relations between privacy and gender have been best described by Anita Allen; cf. for instance Anita LaFrance Allen, 'Still Uneasy: A Life with Privacy', *The Handbook of Privacy Studies* (Amsterdam University Press 2018) 409–412 <https://www.degruyter.com/document/doi/10.1515/9789048540136-021/html> accessed 29 May 2021.
[29] Tracy Higgins, 'Reviving the Public/Private Distinction in Feminist Theorizing Symposium on Unfinished Feminist Business' (1999) 75 Chi.-Kent L. Rev. 847, 847.
[30] Kristin Anne Kelly, *Domestic Violence and the Politics of Privacy* (Cornell University Press 2003).
[31] Danielle Keats Citron, 'Sexual Privacy' (2019) 128 Yale Law Journal <https://digitalcommons.law.yale.edu/ylj/vol128/iss7/2>.

instance been described as both facilitating and impeding the advance of digital rights in India.[32] What we do know is that, in any case, gender matters *de facto* for the enjoyment of privacy and data protection.[33]

Scrutinising women as consumers has been a priority of 'marketing experts' for decades. In this sense, Vance Packard and Mark Crispin Miller already reported in the 1950s about cameras set up in stores that '*started following the ladies as they entered the* store' to measure their eye-blink rate, trying to better understand their behaviour.[34] But women are also scrutinised in other fields, most notably as objects of welfare surveillance.[35] And, as surveillance studies scholars have noted, as a matter of fact volume many '*techniques conventionally relegated to the realm of monitoring and documentation — but not surveillance proper — mask and reinforce the gendered, sexed, raced, and classed exercise of power*',[36]even if society does not generally regard them as proper surveillance. Women suffers from disparate impact even in other more 'protected' environments, like e-commerce.[37]

Gender also significantly matters for the enjoyment of privacy and data protection for trans and gender diverse individuals.[38] The work undertaken by the United Nations (UN) Special Rapporteur on the Right to Privacy in the recent years has notably shown that gender, together with other factors such as ethnicity, beliefs, culture, social origins, age, economic self-sufficiency and legal and political frameworks, serves '*to mould experiences*

---

[32] In this sense, and noting how some concerns about 'protecting women' end up 'reinforcing traditional stereotypes about "fragile, feeble, and dependent" women, widening censorship, and consequently, undermining digital rights': Vrinda Bhandari and Anja Kovacs, 'What's Sex Got to Do with It? Mapping the Impact of Questions of Gender and Sexuality on the Evolution of the Digital Rights Landscape in India – CYRILLA: Global Digital Rights Law' (Cyrilla 2021) <https://news.cyrilla.org/2021/01/new-report-whats-sex-got-to-do-with-it-mapping-the-impact-of-questions-of-gender-and-sexuality-on-the-evolution-of-the-digital-rights-landscape-in-india/> accessed 29 May 2021.

[33] Scott Skinner-Thompson, *Privacy at the Margins* (Cambridge University Press 2021) 39–43 <https://www.cambridge.org/core/books/privacy-at-the-margins/821035ECA5D61516D87C454DD1FF8167> accessed 10 May 2021.

[34] Vance Oakley Packard and Mark Crispin Miller, *The Hidden Persuaders* (Ig Pub 2007) 113.

[35] John Gilliom, *Overseers of the Poor* <https://press.uchicago.edu/ucp/books/book/chicago/O/bo3626685.html> accessed 29 May 2021; See, also, Khiara M Bridges, *The Poverty of Privacy Rights* (1st edition, Stanford Law Books 2017).

[36] Marc Andrejevic, 'Foreword' in Rachel E Dubrofsky and Shoshana Amielle Magnet, *Feminist Surveillance Studies* (Duke Univ Pr 2015) xi.

[37] Will Heilpern, 'Here's how much less women sellers on eBay earn than men' *Business Insider* (26 February 2016) <https://www.businessinsider.com/ebay-gender-pay-gap-exists-2016-2> accessed 20 June 2021.

[38] See e.g. Cayce C Hughes, 'Not Out in the Field: Studying Privacy and Disclosure as an Invisible (Trans) Man' in D'Lane Compton, Tey Meadow and Kristen Schilt (eds), *Other, Please Specify* (University of California Press 2018) <https://www.degruyter.com/document/doi/10.1525/9780520963993-008/html> accessed 29 May 2021; Toby Beauchamp, *Going Stealth: Transgender Politics and U.S. Surveillance Practices* (Duke University Press 2019).

of privacy'.[39] The Special Rapporteur has stressed that *'(g)ender-based breaches of privacy are a systemic form of the denial of human rights, are discriminatory in nature and frequently perpetuate unequal social, economic, cultural and political structures'*[40] and that although *'(p)rivacy and gender have long been regarded as second-order considerations', 'their complex impact on society is of critical importance'*.[41] In general, gender can be a source of vulnerability online for many types of harm: from revenge porn to cyber-harassment and hate speech.[42] Privacy can notably offer protection against gender-based violence, a disturbingly pervasive phenomenon which is known to disproportionately affect women and intersex and gender-nonconforming individuals.[43]

1.4 The role of the GDPR in this debate

In the General Data Protection Regulation (GDPR), the term 'vulnerable data subject' is only incidentally mentioned, referring explicitly just to children. Nevertheless, several European Data Protection Authorities (e.g. in Spain and Poland) have publicly considered 'gender' as a potential source of a data subject's vulnerability. Looking at the history and foundations of European data protection law, broader questions emerge, such as whether the 'average data subject' was or is, by default, male, and, whether females are supposed to be regarded as vulnerable data subjects just because they are female.[44]

This article engages critically with these issues, in line with feminist legal thinking, discusses the recognition of minors as vulnerable (Section 3), by the GDPR, and looks into law and economics analysis of consumers' behaviour (where 'gender' and 'sex' are regarded as a relevant variable in consumer vulnerability) (Section 2), but also political philosophy and, in particular, gender studies (Section 4), where we can observe a real intellectual polarisation. On the one hand the vulnerability universalist approach,[45] according to which

---

[39] United Nations (UN) General Assembly, 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development, A/RES/75/176' 4.
[40] ibid., 3.
[41] ibid., 4.
[42] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) <https://www.jstor.org/stable/j.ctt7zsws7> accessed 29 May 2021; Michele E Gilman and Rebecca Green, 'The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization' (2018) 42 NYU Review of Law and Social Change 253; Lori Janjigian, 'Nearly 10 Million Americans Are Victims of Revenge Porn, Study Finds' *Business Insider* (13 December 2016) <https://www.businessinsider.com/revenge-porn-study-nearly-10-million-americans-are-victims-2016-12> accessed 20 June 2021.
[43] United Nations (UN) General Assembly (n 38) 4; See, also, Citron (n 41); Carrie Goldberg and Jeannine Amber, *Nobody's Victim: Fighting Psychos, Stalkers, Pervs, and Trolls* (Plume 2019).
[44] Conceptualisations that would be based on an approach to gender different than binary are difficult to find in the doctrine.
[45] Judith Butler, *Precarious Life: The Powers of Mourning and Violence* (Verso 2006); Fineman (n 22); Catriona Mackenzie, Wendy Rogers and Susan Dodds (eds), *Vulnerability: New Essays in Ethics and Feminist Philosophy* (1 edition, Oxford University Press 2013).

every human is vulnerable and any additional 'label' of vulnerability is deemed to lead only to stigmatisation and 'pathogenic vulnerability'; and, on the other hand, the particularistic approach,[46] according to which some subjects are more vulnerable than others (and, in particular, women are more vulnerable – i.e. subject to adverse effects – than men in many contexts: workplace, education, etc.). A third way might be the 'layered' theory of Luna,[47] which is based on a contextual and relational (even situational) nature of vulnerability. This solution could be regarded as best adapted to the layered risk-based approach in the GDPR, but also with intersectional approaches.[48] In addition, as Section 5 highlights, this contextual approach is somehow present also in new policymaking proposals, although we should be aware of its inherent risks too (Section 6).

2. Engendering the (average) data subject?

2.1 The average data subject in the GDPR

While in EU data protection law there are clear definitions of key notions such as 'data controllers' and 'data processors', and these might even be classified into different categories (according to size, responsibility, data protection risks, territoriality, etc.),[49] not much can be said about data subjects.[50]

Data subjects are defined in the GDPR indirectly, in the definition of personal data of Article 4(1), which states that '*"personal data" means any information relating to an identified or identifiable natural person ("data subject")*'. The data subject is thus the identified or identifiable natural person to whom personal data relate. Nothing is said about the main characteristics of this legal figure, although one could attempt to re-construct such main characteristics from the other provisions of the GDPR. In this sense, for instance, the data subject would appear to be, in principle, somebody who is unaware of the existence of their data protection rights – as the GDPR obliges data controllers to inform data subjects

[46] Goodin (n 8); Cole (n 15).
[47] Luna, 'Elucidating the Concept of Vulnerability' (n 25); Luna, 'Identifying and Evaluating Layers of Vulnerability – a Way Forward' (n 25).
[48] Understanding intersectionality as a prism to acknowledge 'overlapping vulnerabilities'. See Kimberlé W Crenshaw, 'From Private Violence to Mass Incarceration: Thinking Intersectionally about Women, Race, and Social Control' (2013) 9 Journal of Scholarly Perspectives 23 <https://escholarship.org/uc/item/7mp3k6m3> accessed 29 May 2021.
[49] See, in particular, Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia Uitgevers N V 2019).
[50] Peter Blume, 'The Data Subject' (2015) 1 European Data Protection Law Review 258; See, more recently, Aisha PL Kadiri, 'Data and Afrofuturism: An Emancipated Subject?' (2021) 10 Internet Policy Review <https://policyreview.info/articles/analysis/data-and-afrofuturism-emancipated-subject> accessed 5 May 2022.

about these rights whenever they collect data from them (cf. Art. 13 GDPR). At the same time, in principle, data subjects are nevertheless expected to be able to provide – after having received certain pieces of information – a consent that qualifies as informed. The data subject is thus in principle uninformed, but potentially on the verge of being informed enough.[51]

EU data protection law does not explicitly rely on the notion of 'average data subject'[52] or put forward any comprehensive classification of data subjects. As it does refer to vulnerable data subjects, it is possible to state all other data subjects are thus to be regarded as non-vulnerable. To some extent, it is possible to equate the ideal 'average data subject' to such category of non-vulnerable data subjects. In any case, what we know about vulnerable data subjects is that they are not the standard data subject.

In many other EU legal fields, there are more specific definitions of the different individuals involved and possible sub-categories of them. This is the case in such as EU private law, consumer law,[53] car insurance regulation,[54] and regulation of scientific research.[55] For example, in these fields there are descriptions of *average* subjects and separate descriptions of *vulnerable* individuals (classified either generally or on the basis of the specific groups they belong to). Still, in the data protection framework, in which these definitions, distinctions and categorisations could seem even more important, they are absent.

2.2 From the Data Protection Directive to the GDPR: a rational male subject?

If we understand privacy and data protection law as aimed at counter-balancing unfair imbalances between the data processing party and the data subject,[56] they could be described as thus aimed at mitigating individual vulnerability.[57] However, the increased

[51] On the relation between the notion of data subject and information, see notably Gloria González Fuster, 'How Uninformed Is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection' (2014) 19 IDP Revista de Internet, Derecho y Política 92.
[52] ibid.
[53] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance) 2005 [32005L0029].
[54] 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.
[55] See, e.g. 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 2014 (OJ L).
[56] See Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 213.
[57] Ryan Calo, 'Privacy, Vulnerability, and Affordance' (2017) 66 DePaul Law Review <https://via.library.depaul.edu/law-review/vol66/iss2/11>.

awareness in social science about the dynamic personal conditions of individuals (in terms of understanding, awareness, exposure to manipulation and discrimination, resilience to attacks, etc.)[58] impose to consider that there exist different layers of data subjects' vulnerability. In the GDPR (and in the Data Protection Directive before) it is clear that some rules are conceived for 'average' (rational, aware and circumspect) data subjects.

Indeed, as many scholars affirm, the emphasis on information duties in the data protection discourse presupposes a rational, informed data subject who makes conscious decisions.[59] The emphasis on consent, as the outcome of a rational and informed decision-making process of the data subject, reflects the same approach. Interestingly, if we look back at the first proposal of the Commission for the Data Protection Directive, we can find several references to a rational and well-informed average data subject. In particular, the right to information is seen as a tool to 'enable the data subject *to weigh the risks and advantages of the intended processing* of data relating to him and to exercise his rights under Article 14 of the Directive (rectification, erasure, blocking)'; accordingly 'the controller of the file has to provide the data subject with such information as is relevant to the data subject's decision'.[60] In other words, the legislator was relying on the rational decision-making capabilities of the data subject, who is able to assess risks and advantages of data processing and to take informed decisions about that. She seems similar to the reasonably informed, observant and circumspect consumer that can 'make intelligent choices' as argued in the consumer law *acquis*.[61]

According to some commentators, the shift from the Data Protection Directive to the GDPR has not decreased but increased this reliance on an average and rational data subject, inspired to the rational consumer in the EU consumer law. In particular, considering the new emphasis on the characteristics of valid *consent* (Article 7),[62] the introduction of *transparency* as an explicit data protection principle (Article 5(1), point (a)) and the consequent development of information duties (see Articles 12-14), it seems that the

---

[58] See, e.g. Martie G Haselton, Daniel Nettle and Paul W Andrews, 'The Evolution of Cognitive Bias' in David M Buss (ed), *The Handbook of Evolutionary Psychology* (John Wiley & Sons, Inc 2015) <http://doi.wiley.com/10.1002/9780470939376.ch25> accessed 28 February 2019.

[59] 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' (2014) 16 Ethics and Information Technology 171, 171; González Fuster (n 50).

[60] Commission of the European Communities, Communication on the protection of individuals in relation to the processing of personal data in the Community and information security; Proposa1for a Council Directive concerning the protection of individuals in relation to the processing of personal data Draft, COM(90) 314 final, SYN 287 and 288, Brussels, 13 September 1990, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990DC0314&from=EN, 26.

[61] *Esteé Lauder Cosmetics GmbH & Co. OHG v. Lancaster Group GmbH*, Opinion of Advocate General Fennelly delivered on 16 September 1999, C-220/98, ECR, 2000, I–117.

[62] About the paradoxical effect of the new emphasis of consent in the GDPR see Joris van Hoboken, 'The Privacy Disconnect' in Rikke Frank Jørgensen (ed), *Human rights in the age of platforms* (The MIT Press 2019) 266, 268.

GDPR is '*based on the idea that all data subjects are rational actors that will read all privacy statements and carefully weigh and balance the consequences of consent*'.[63]

Actually, some provisions in the GDPR seem to refer to a broad notion of data subject, which may include also vulnerable subjects. This is the case of, e.g., Article 12 that requires that the data controller complies with all transparency duties in an '*intelligible and easily accessible form, using clear and plain language*'. We can find another reference to this in Recital 43, which affirms that the provision of consent is probably not free if there is a 'clear imbalance between the data subject and the controller'. Another implicit reference is in Article 21(1), according to which the right to object should be exercised on grounds relating to the data subject's 'particular situation'. Other references to vulnerable individuals can be found in the notion of 'high-risk' data processing (Recital 75) or in the exercise of some data protection rights (e.g. the right to be forgotten or the right not to be subject to automated decisions).[64] Actually, in most of these few examples, the only explicit reference to vulnerable subjects in the GDPR is to children, as we discuss in the next section (Section 3).

In more general terms, several scholars have criticised the normative definition of the 'average' individual in law, seen as a tool to strengthen dominant categories (white, male, heterosexual, upper classes individuals) and stigmatise minority or vulnerable groups,[65] while others have noted that the liberal legal person is marked – historically or normatively – by inherent masculinity.[66]

In privacy and data protection discussions, there is no definite understanding or clear classification of vulnerable individuals,[67] but also no generally accepted conceptualisation of the standard data subject. By exploring the operationalisation of vulnerability in data protection law, however, we can throw light on who is supposed to be, *a contrario*, the standard data subject. In Europe, privacy and data protection legislation has never clarified the gender of the non-vulnerable data subject. The text of the 1995 EU Data Protection Directive refers to the data subject using male pronouns (he/him). However, that was a common linguistic bias in that period. Interestingly, the figure below, reproducing a

---

[63] Schermer, Custers and van der Hof (n 58) 179.
[64] See article 17(1)(f) about the right to be forgotten for children or recital 71 about the right to be subject to automated decision-making and the prohibition of these automated decisions for children.
[65] Mayo Moran, *Are Objective Standards Worth Saving? Exploring the Feminist Debate* (Oxford University Press 2003) <https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199247820.001.0001/acprof-9780199247820-chapter-7> accessed 9 March 2020; Ngaire Naffine, *Law and the Sexes: Explorations in Feminist Jurisprudence* (Allen & Unwin 1990).
[66] Rosemary Hunter, 'Contesting the Dominant Paradigm: Feminist Critiques of Liberal Legalism' in Margaret Davies and Vanessa Munro (eds), *The Ashgate Research Companion to Feminist Legal Theory* (Ashgate 2013) <https://kar.kent.ac.uk/35679/> accessed 29 May 2021.
[67] Malgieri and Niklas (n 1).

fragment of a figure from a European Commission document of 1998,[68] offers a gendered representation of the data subject, might also be regarded as plausibly standard for that period.

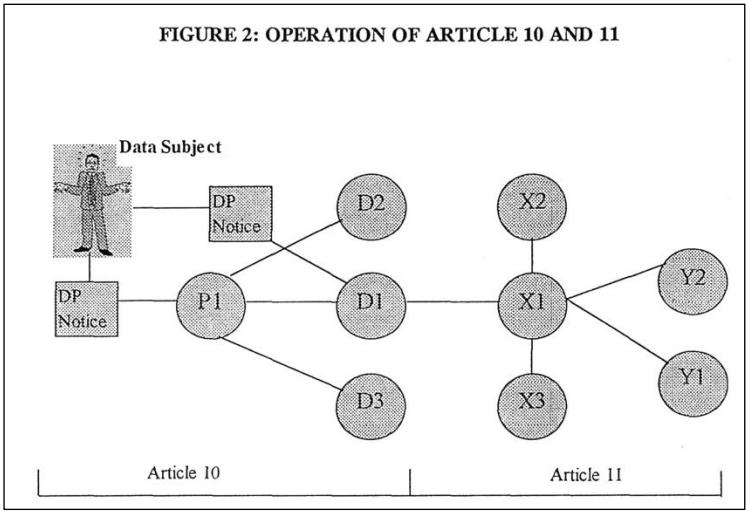

Figure 1 – Example of historical representation of the data subject

Nevertheless, the GDPR, that repealed that Directive in 2016, has more gender-neutral terminology: it always refers to 'he or she'/'him or her'. Indeed, European data protection law is overall not concerned with gender.[69] This GDPR gender 'blindness' is manifest in relation to the categories of data protected as 'special categories' or 'sensitive data'. Article 9(1) GDPR, which establishes that in principle data pertaining to such categories shall not be processed, does not mention gender (or even gender identity) or sex among the types of sensitive information that must be specially protected because they could, *inter alia*, lead to discrimination.

[68] European Commission (1998), *Handbook on cost-effective compliance with Directive 95/46/EC*, DG XV – Internal Market and Financial Services.

[69] This is particularly striking in light of the described significance in relation to privacy and personal data processing, although this is not as such as peculiarity of data protection law, and gender might be described as overall 'barely visible in the conceptual armoury of law'. See Joanne Conaghan, *Law and Gender* (Oxford University Press 2013).

2.3 The role of Data Protection Authorities in 'inventing' the vulnerable gendered data subject

More broadly, it has been highlighted that not only European but more generally all worldwide data protection authorities tend to disregard the issue of gender, notably when they record and report on their interactions with data subjects.[70] Because of such lack of gender-sensitive reporting, it is difficult, not to say impossible, to have an accurate understanding of the extent to which gender affects access to data protection remedies.

A link between gender and data protection vulnerability has been suggested however by some EU Data Protection Authorities. It is the case of, at least, Spain and Poland. The Spanish DPA has notably argued in its 2020 gender equality framework that ongoing technological changes impact all citizens but especially 'the more vulnerable collectives, like children and women'.[71] On the other hand, the Polish Data Protection Authority, in its list of high-risk data processing practices (for which a Data Protection Impact Assessment should be recommendable), mentions gender as a source of power imbalance in data-related contexts: 'processing data in which the data subjects are graded or assessed, e.g. in terms of age and/or *gender*, and then this classification is used to present offers or other activities that may affect the rights and freedoms of data subjects whose data are processed.'.[72] In sum, gender and vulnerability are linked on the grounds of consumer and worker exploitation. In other terms, the Polish DPA seems to suggest that non-male gender might lead to contractual vulnerability, as many national civil codes have been also suggesting during the 20th century.[73]

Interestingly, in the consumer law and economics literature, the link between vulnerability and gender has been discussed in different empirical studies. For example, women appear to score lower on the consumer empowerment index than men[74] and gender could be seen

---

[70] Elizabeth Coombs and Kara McKee, 'The "Missing Women" in Data Protection Reporting' <https://iapp.org/news/a/the-missing-women-in-data-protection-reporting/> accessed 29 May 2021.

[71] Translated by the authors. The original states: 'La protección de datos vive un momento determinante debido a los continuos cambios tecnológicos que impactan directamente en el ciudadano y en especial en los colectivos más vulnerables como los menores y las mujeres que nos conciencian, entre otras cosas, de que es necesario luchar contra la violencia en internet' (AEPD, *Marco de Actuación de la Agencia Española de Protección de Datos en materia de Igualdad de Género*, 2020, p. 3).

[72] Proponowany wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych, https://iapp.org/media/pdf/resource_center/poland_blacklist.pdf.

[73] See the Italian Civil Code Art. 1435, according to which the use of violence during the negotiations for a contract can be a cause of invalidity of the contract. 'The violence must be of such a nature as to make an impression on a reasonable person and to make him fear exposing himself or his property to an unjust and considerable evil. Regard shall be had, in this matter, to the age, *sex* and condition of persons'.

[74] M Nardo and others, 'The Consumer Empowerment Index. A Measure of Skills, Awareness and Engagement of European Consumers' [2011] Publications Office of the European Union 12

as directly linked to vulnerability for instance in situations where men control women's access to money.[75] Obviously, significant life changes experienced by some women, such as pregnancy, can be sources of certain types of vulnerability.[76] In addition, men tend to dominate the use of new technologies such as internet banking, resulting in potential vulnerability in the online and financial sectors being determined along gender lines.[77]

A European Commission study on consumer vulnerability in 2016[78] revealed that men appear consistently less likely than women to be 'vulnerable' on a number of indicators in the commercial dimension. The indicators included having problems comparing deals due to personal, market-related and access-related factors in the energy sector, due to personal and market-related factors in the online sector, and due to personal and market-related factors in the finance sector, as well as being prevented from switching due to access-related factors in the energy sector.

The study also highlighted that vulnerability is not always connected to the female gender: according to the results of the survey data analysis, men are slightly more likely to not take action when they experience a problem, and to overpay for services due to being unable to use certain payment methods.[79]

2.4 The gendered subjectivity paradox in the privacy discourse

At this stage, it is necessary to stress that when legal texts or authorities refer to vulnerability in these contexts, they may refer to two different kinds of vulnerability: vulnerability as being particularly vulnerable *to the effects* of data processing (higher risk of discrimination, manipulation, stigmatisation, physical or psychological harm, etc.) and vulnerability *within* the data processing process itself (higher risk of not understanding privacy policies, not providing an aware and voluntary consent to data processing, not understanding risks and implications of it, being incapable of exercising data protection rights).[80] Women are usually portrayed to as especially vulnerable *to the effects* of data processing (discrimination in the workplace, harassment on social media, etc.), but often

</paper/The-consumer-empowerment-index.-A-measure-of-and-of-Nardo-Loi/351cd8a65375fa006fd18acc342741aab2a65a14> accessed 10 May 2021.

[75] Elizabeth Branigan and Marty Grace, 'His Money or Our Money: Financial Abuse of Women in Intimate Partner Relationships' [2005] Coburg, Vic: The Coburg Brunswick Community Legal and Financial Counselling Centre Inc <https://core.ac.uk/display/36837980> accessed 10 May 2021.

[76] The VOICE Group, 'Motherhood, Marketization, and Consumer Vulnerability' (2010) 30 Journal of Macromarketing 384.

[77] Jan Pahl, *Invisible Money: Family Finance in the Electronic Economy* (Policy Press 1999).

[78] European Commission, 'Consumer Vulnerability across Key Markets in the European Union' (2016) <https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf>.

[79] ibid.

[80] About this distinction of two kinds of vulnerabilities, see largely Gianclaudio Malgieri, 'Data Subjects in the GDPR and the Protection of Vulnerable Individuals' (Doctoral Thesis, Vrije Universiteit Brussel 2020).

the distinction between these two forms of vulnerability is blurred or conceptually confused, as for the case of children, mentioned below in this article.

However, the fact that women are considered vulnerable to the effects of data processing, rather than vulnerable in reading privacy documents or exercising data subjects' rights is emblematic. Indeed, in the previous sections we have observed a paradox about privacy subjectivity and gender: women are considered as privacy subjects when they need to be 'protected' against the effects of data protection,[81] but, at the same time, the average data subject – the one that actively reads privacy policies and takes decisions, gives consent, exercises data protection rights – seems to be implicitly *male* by default. In other words, women have been considered as 'objects' of privacy, but not as 'subjects' of privacy. The sexist dichotomy objects-subjects or Self-Other has been well explored in feminist studies,[82] building on Simone De Beauvoir reflections.[83] Although a comprehensive comparison between that discussion and the privacy gendered subjectivity paradox is beyond the scope of this article, we acknowledge that even the privacy discourse has tended to consider 'men' as data protection *subjects* (see the EU Data Protection Directive above) and 'women' as data protection *objects* (see the link between female gender and vulnerable subjects above).

3. The problem of labels in the data protection discussion on vulnerability

3.1 Children as vulnerable data subjects

One of the main risks of defining and addressing vulnerable data subjects is the risk of labelling them, stigmatising minorities and oversimplifying complex dynamics. By doing so, whole groups of individuals are moved out of standard legal protection into a realm which is not necessarily better fitted to tackle the issues at stake. A clear example of these risk is the protection of children as the only explicit vulnerable category of data subjects in the GDPR.

Indeed, the GDPR recognises explicitly only one category of vulnerable individuals (cf. Recital 75): children. Analysing the GDPR consideration and protection of children's vulnerability can thus be useful to better understand also how such an approach can be

[81] Allen and Mack (n 3); Skinner-Thompson (n 4).
[82] Karen Green, 'The Other as Another Other' (2002) 17 Hypatia 1, 6–9; Céline Léon, 'The Second Sex: Differently Other or Otherly Different?' (1995) 12 Simone de Beauvoir Studies 139, 141; Sonia Kruks, 'Gender and Subjectivity: Simone de Beauvoir and Contemporary Feminism' (1992) 18 Signs 89.
[83] Simone De Beauvoir, *The Second Sex* (Constance Borde and Sheila Malovany-Chevallier trs, 1st edition, Vintage 2011) 44, 120, 152.

put in relation to the discussion about gender vulnerability. This section analyses, therefore, the qualification by the GDPR of children as vulnerable data subjects, and the special rules put in place for the protection of the personal data about them. It briefly considers the reasons behind such a move, stresses that the rationale for that decision was originally ill-defined, and highlights that, in practice, it has not led to reinforced protection of the personal data of children. On the contrary, it might be argued that as a consequence of the special rules foreseen in the GDPR for the processing of minors' data, minors are now in a particularly uncomfortable and dangerous situation – notably due to what we describe as the 'Frosties effect' (see below).

The GDPR was the first EU legal instrument to recognise that minors deserve *'specific protection'* of their personal data.[84] This is due, according to the GDPR, to the fact that '*they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*'.[85] The Regulation also explicitly mentions children as a type of '*vulnerable natural persons*', in the sense that the risk to their rights and freedoms of resulting from personal data processing might be particularly likely and severe.[86] The rationale for treating minors differently seems thus to be at least double: it is because they know less than normal adults, and it is because the impact of data processing can be worse for them. The EU legislator was never completely clear in this respect during the legislative procedure.[87]

The lack of clear argumentation in this regard was particularly visible in discussions around the age below which data subjects cab only consent via 'parental consent'. Article 8(1) of the GDPR, in this sense, establishes that, *'in relation to the offer of information society services directly to a child'*, the processing of the personal data of a child below the age of 16 years shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. The GDPR does not explain however exactly why consent of younger children should not be valid. It might be that they are too young to be properly informed, and thus incapable of granting 'informed consent' because of their limited knowledge. It might be that due to their limited age there is, as a general rule, a 'clear imbalance' between them and the data controller, imbalance which would also invalidate the possibility of consent. It might be that the impact on them of certain data practices would potentially be too severe, and thus they are especially at risk, in a way that would make their own consent a non-suitable legal basis. It might be that the reasoning behind the measure builds on all of these points. No explanation is given.

The absence of clear criteria to determine the consent threshold eventually affected negatively national developments, which have happened to be extremely uncoordinated and diverse. Article 8(1) of the GDPR indeed also opened the door for Member States to '*provide by law for a lower age for those purposes provided that such lower age is not below 13 years'*, that is, to decide by themselves what would be the exact threshold for parental

[84] Recital (38) of the GDPR.
[85] Idem
[86] Recital (75) of the GDPR.
[87] See Gloria González Fuster, 'GDPR: We All Need to Work at It!' (*Better Internet for Kids*, 31 March 2016) <https://www.betterinternetforkids.eu/practice/articles/article> accessed 29 May 2021.

consent in their territory. Member States ended up setting the threshold at a variety of different ages, including 13, 14, 15 and 16 years.[88] This created a not clearly justified, not to say random, normative fragmentation directly at odds with the harmonising ambitions of the GDPR.

Worse, the need to comply with special requirements in the event that Article 8 GDPR would apply, combined with the need to adapt to national disparate norms, appeared to motivate a global move from data controllers to situate themselves out of its reach. We designate this phenomenon as the 'Frosties effect', in relation to accusations addressed at Kellogg's UK when the company, having to face limitations of sugar content in cereals addressed to children, decided to announce that its Frosties cereals did not target children.[89] The decision was controversial because the product is typically associated with a cartoon mascot. Nevertheless, the company insisted that Frosties tended to be eaten by more adults than children.

In a similar vein, companies that one could imagine as targeting children, assert nowadays that they do not. Also, often, data controllers will use data protection notices to announce that actually minors should actually be kept away from them. In this sense, for instance, Fanta states that in Belgium nobody younger than 16 can participate to activities requiring consent – not even with parental consent.[90] As another example, TikTok asserts it is not for children younger than 13, and places on the readers of their data protection notices the burden of notifying any possible access to personal data of minors.[91]

By artificially negating that they target children, data controllers might be trying to avoid having to comply with Article 8 of the GDPR. *De facto*, they sometimes pursue avoidance in a way that actually completely refutes the possibility that data about children might be processed at all by them, depriving children of even basic data protection safeguards. In its assessment of the first two years of application of the GDPR, the European Commission, despite providing a generally positive evaluation of the instrument's application, was highly critical of the situation regarding the protection of personal data of children.[92] The

---

[88] Ingrida Milkaite and Eva Lievens, 'Status Quo Regarding the Child's Article 8 GDPR Age of Consent for Data Processing across the EU' (*Better Internet for Kids*, 20 December 2019) <https://www.betterinternetforkids.eu/practice/articles/article> accessed 29 May 2021.

[89] Jamie Grierson, 'Kellogg's UK Prompts Anger by Branding Frosties an Adult Cereal' *the Guardian* (1 December 2017) <http://www.theguardian.com/society/2017/dec/01/kelloggs-uk-anger-branding-frosties-adult-cereal-sugar> accessed 29 May 2021.

[90] '*Cela signifie que les personnes âgées de moins de 16 ans ne peuvent pas participer aux activités énumérées à l'article 6 lorsqu'elles sont fondées sur le consentement, par exemple recevoir des communications marketing et des notifications push personnalisés en fonction du lieu, et que nous ne traitons pas leurs Données Personnelles*', https://promo-fr.fanta.be/politique-de-confidentialite, accessed 13 April 2021.

[91] '*TikTok n'est pas destiné aux enfants de moins de 13 ans. Si vous pensez que nous avons des données personnelles concernant un enfant ou collectées auprès d'un enfant n'ayant pas l'âge requis, veuillez utiliser le formulaire situé à l'adresse*', https://www.tiktok.com/legal/report/privacy, accessed 13 April 2021.

[92] European Commission, *Communication to the Council and to the European Parliament: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two*

European Commission notably noted that national differences in the age of children's consent in relation to information society services create '*uncertainty to children and their parents as to the application of their data protection rights in the Single Market*'.[93] The document accompanying the official Communication of the European Commission also pointed out that one of the areas in which further progress was needed was the rights of children, echoing concerns that *'many organisations ignore that children may be concerned by their data processing'*.[94]

In sum, providing specific protection for the personal data of children – explicitly identified as vulnerable – was a significant innovation of the GDPR, but it has been, for the moment, one of its most dramatic failures. The data of children have not only not received particularly strong protection. They have actually received a level of protection particularly weak, and often completely ignored.

3.2 Layered vulnerability as an alternative interpretation of the GDPR

Considering and addressing data subjects' vulnerability is important and even necessary. However, considering a risk-based definition of vulnerability (vulnerability as higher risks to people's fundamental rights and freedoms), we should not assume that groups are 'vulnerable' by default. On the contrary, vulnerability should be analysed under a contextual, relational and intersectional approach.

As explained above, Luna, trying to conciliate the risk-based approach of vulnerability with a relational and intersectional understanding of vulnerable people, proposes the notion of 'layered' vulnerability.[95] In sum, she does not consider human vulnerability as a yes-or-no attribute, but as a risk-based characteristic of individuals, depending on the geographic, socio-economic, institutional, structural and hierarchical conditions in which a powerless data subject is. This layered-based approach to human vulnerability seems adequate to avoid default considerations ('children are vulnerable', 'women are vulnerable') and

years of application of the General Data Protection Regulation, COM(2020) 264 final, Brussels, 24.6.2020.

[93] Ibid., p. 16.

[94] European Commission, *Commission Staff working document accompanying the Communication to the Council and to the European Parliament: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the General Data Protection Regulation*, COM(2020) 264 final, Brussels, SWD(2020) 115 final. In light of this assessment, the European Commission invited data protection authorities (hereafter: DPAs) to adopt guidelines on the processing of children's data (COM(2020) 264 final, p. 16) and committed to '*provide for tools clarifying/supporting the application of data protection rules to children*' (ibid., p. 7) but also to explore whether it might be appropriate to propose possible future targeted amendments to certain provisions of the GDPR, notably for a possible harmonisation of the age of children's consent in relation to information society services (ibid., p. 15).

[95] Luna, 'Elucidating the Concept of Vulnerability' (n 25); Luna, 'Identifying and Evaluating Layers of Vulnerability – a Way Forward' (n 25).

embrace more contextual and relational understandings of vulnerability (e.g. 'a woman who is a precarious worker for a digital platform of food delivery is vulnerable when her employer asks for her consent for the access to health data on her mobile phone', etc.).

Interestingly, this layered-approach is really in line with the risk-based approach in the GDPR. Indeed, as some scholars affirmed, the layers assessment in Luna's theory is a specific form of risk assessment.[96] The link between vulnerability and risk is also semantic, as the first definition of 'risk' in data protection reveals ('exploitation of vulnerability of personal data supporting assets').[97]

In other terms, vulnerability should not be considered as a static, immutable property of 'categories' (or groups) of data subjects, but as a dynamic and relational risk-based attribute of data subjects in certain situations. The GDPR is already compatible with this structure. Interpreters should avoid default interpretations of vulnerabilities ('children are vulnerable') and conjugate the risk-based approach of articles 24 (the duties of the data controller should be proportional to risks), 25 (data protection by design should take into account the level of risks) and 35 (the DPIA focuses on risks for data subjects) to a dynamic understanding of vulnerability.[98]

Accordingly, the risk-based approach seems fruitful for our study on vulnerability. When assessing the risks to fundamental rights and freedoms of the data subjects, the data controller should consider situations in which certain data processing could adversely impact particular individuals. This is explicitly requested by the WP29, which declared that 'origin, nature, particularity and severity of the risks' should be appreciated '*from the perspective of the data subjects*'.[99] Indeed, this approach has been defined as 'subjective, individual-centred'.[100] In sum, even though the GDPR is not clear and unambiguous in defining and protecting vulnerable people, the interpreters should treasure the risk-based approach in order to face the challenge of vulnerable data subjects and avoid ex-ante oversimplified understandings of data subjects' vulnerabilities.

---

[96] See Gennet, Andorno and Elger (n 20).

[97] CNIL, 'Privacy Impact Assessment (PIA) – Methodology (how to carry out a PIA)' (2015) 6 <https://www.cnil.fr/sites/default/files/ typo/document/CNIL-PIA-1-Methodology.pdf. See also István Böröcz, 'Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras' (2016) 2 European Data Protection Law Review 467.

[98] Malgieri and Niklas (n 1).

[99] WP29 Guidelines on DPIA, 21. Emphasis added. See also, on this point, Katerina Demetzou, 'Risk to the "Rights and Freedoms" – A Legal Interpretation of the Scope of Risk Under the GDPR', in Ronald Leenes et al., *Data Protection and Privacy*, Bloomsbury, 2020.

[100] Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8 European Journal of Risk Regulation 506, 536.

4. New frontiers in policymaking: from vulnerable individuals to individuals with vulnerabilities?

The contextual approach according to which vulnerability is not a static attribute of a category of individuals (e.g. women), but a transient and contextual situation depending on the specific circumstances of the data processing can be found also in international and EU policy documents,[101] as well as guidance from data protection authorities. For example, the Spanish DPA,[102] in its official list of high-risk data processing practices, mentioned: 'data processing regarding vulnerable subjects or those who are at risk of social exclusion, including (…) the victims of *gender-related violence*, as well as their descendants and persons who are in their guardianship or custody'.[103] Victims of gender-related violence might be regarded as vulnerable due to their gender, but this is not here a general assumption according to which women are vulnerable: it is rather a contextual evaluation (gender can be a source of domestic violence or similar forms of violence and so a source of vulnerability).

Somehow similarly, the UN Special Rapporteur on the Right to Privacy refers to individuals '*vulnerable on account of their gender*', but in our interpretation at least these do not necessarily correspond to all individuals of a certain gender.[104] Rather, these would be individuals who have suffered 'infringements of privacy related to or arising from' their gender.[105]

A layered approach – described as a possible solution in the previous Section – could be read between the lines of the proposed EU legislation on AI. In this sense, the recently proposed EU AI Act[106] in its Article 5 mentions 'people with vulnerabilities', instead of 'vulnerable people'. This idea of vulnerabilities as an eventual (and transeunt) adjective seems very in line with a 'layered' approach to vulnerable subjects.[107] Another passage of

---

[101] It might worth noting that in the EU context 'vulnerable adults' is used to describe persons lacking the personal capacity to protect their interests. See for instance: Christian Salm, *Protection of Vulnerable Adults: European Added Value Assessment Accompanying the European Parliament's Legislative Initiative Report (Rapporteur: Joëlle Bergeron) : Study* (EPRS, European Parliamentary Research Service, European Added Value Unit 2016) 388.

[102] AEDP, List of the types of data processing that require a data protection impact assessment under Art 35.4, English version available here: https://www.aepd.es/media/criterios/listas-dpia-en-35-4.pdf

[103] See on this point, e.g. Erinn Gilson, *The Ethics of Vulnerability: A Feminist Analysis of Social Life and Practice* (1 edition, Routledge 2014) 148–177.

[104] *Report of the Special Rapporteur on the right to privacy*, op. cit., p. 4.

[105] Gender being understood here as encompassing *'(c)is normativity, biological sex, sexual orientation and expression, gender identity or expression, sex characteristics and societal norms'* (idem).

[106] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts {sec(2021) 167 final}, Brussels, 21 April 2021.

[107] It is unclear and very much subject to debate, however, whether this might be a deliberate and conscious choice from the services drafting the proposal, or rather an accidental consequence of the fact that there are the same services normally working on cybersecurity legislation, in which the term 'vulnerabilities' is most common.

the AIA proposal also refers to vulnerability, in this case demanding that attention is paid to a possible '*vulnerable position'* in which adversely impacted persons might find themselves in relation to the user of an AI system, '*in particular due to an imbalance of power, knowledge, economic or social circumstances, or age'*. This vulnerable position of impacted persons needs to be taken into account for assessing the possible future qualification of additional AI systems as high-risk systems, under the proposed Article 7(2)(e). Actually, the European Commission's approach to vulnerability is not particularly consistent. In its Communication of December 2020 on the *Digitalisation of justice,*[108] the European Commission notes that 'the digitalisation process must take full account of the needs of the disadvantaged groups', and that 'institutional, organisational and technical measures must ensure full access to justice by *disadvantaged groups and people in situation of vulnerability, such as children or older people*, who may lack the requisite means or digital skills'.[109] This seems to imply a distinction between people pertaining to a 'disadvantaged group', and people 'in situation of vulnerability', where only age is mentioned as an example of vulnerability source (but, e.g. disability – which is in Article 5 of the proposed regulation on AI – is not here). The same Communication, when it moves to considering AI developments, states that where 'machine learning is used, the risks of biased outcomes and potential discrimination against *women and particular groups,* such as persons with a minority ethnic or racial background, are high and must be addressed'.[110] Here the terminology privileged is thus 'women and particular groups', as if the Commission wanted to keep anyway a more static approach on 'group' vulnerability and 'women' are seen at the borderline of these special groups.

In its 2020 Strategy on Gender Equality,[111] when discussing women's employment rate in the EU, the European Commission stated that there was an underrepresentation of some women in the labour market which is '*often resulting from the intersection of gender* with additional conditions of vulnerability or marginalisation[112] *such as belonging to an ethnic or religious minority or having a migrant background*',[113] thus equating being a woman with a condition of vulnerability. The 2020 European Commission's Strategy for lesbian, gay, bisexual, trans, non-binary, intersex and queer (LGBTIQ) people,[114] in its turn, generally regarded LGBTIQ people as a vulnerable group but also noted that among LGBTIQ people some are '*the most vulnerable'*, in particular *'those experiencing intersectional*

---

[108] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitalisation of justice in the European Union A toolbox of opportunities*, COM(2020) 710 final, Brussels, 2.12.2020.

[109] Ibid., 5. Emphasis added.

[110] Ibid., 11. Emphasis added.

[111] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Union of Equality: Gender Equality Strategy 2020–2025*, COM(2020) 152 final, Brussels, 5.3.2020.

[112] Emphasis added.

[113] Ibid., 7.

[114] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Union of Equality: LGBTIQ Equality Strategy 2020–2025*, COM(2020) 698 final, Brussels, 12.11.2020.

discrimination and trans, non-binary and intersex people, who are among the least accepted groups in society and generally experience more discrimination and violence than others in the LGBTIQ communities'.[115]

The European Data Protection Supervisor (EDPS), commenting in June 2020 on the European Commission's approach to AI,[116] suggested in that '*in the absence of a formally adopted legal definition of vulnerable groups'*, '*a context-specific, pragmatic approach'* should be adopted.[117] This statement, however, was followed by an enumeration of groups of persons to be regarded as vulnerable, and thus the 'context-specificity' of the approach is unclear: *'Vulnerable group [sic] of persons should include children, elderly, and persons with disabilities, ethnic minorities or historically marginalised groups*, women,[118] *LGBTQIA+ communities, workers and others at risk of exclusion'*.[119]

In sum, it seems to us that in the guidelines and institutional documents in the EU there is an ambiguous but intense focus on individual vulnerability: we observe a tension between static group vulnerability (in which often gender is considered a source of vulnerability) and dynamic, contextual approach to vulnerability as a transeunt adjective of individuals. In our view, this tension could benefit from the feminist and gender studies discussion summarised in the previous sections: a layered approach to vulnerability might be a first solution to protect people, without stigmatising them, and facilitate the acknowledgement of the possible coexistence of multiple vulnerability layers.

5. The risk of layerism: the contextual invalidation of vulnerability

This contextual recognition of vulnerability, however, is not without risks, the most important being that it might generate situations in which an individual expecting to be granted special protection is deprived of it because, taking into account their specific situation and despite possible appearances, they are individually regarded as not being vulnerable. Again, minors can provide here a useful illustration – minors being, as noted, currently the only category of explicitly vulnerable data subjects in the GDPR. Particularly telling is the case connected to Decision n° 53 of the European Data Protection Board (EDPB) Register of Decisions taken under Article 60 of the GDPR.[120] The decision relates to a complaint lodged by a 15-year-old individual with the Austrian Data Protection Authority,

[115] Ibid., 3.
[116] European Data Protection Supervisor (EDPS), *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*, June 2020.
[117] Idem, 21.
[118] Emphasis added.
[119] European Data Protection Supervisor (EDPS), *Opinion 4/2020,* 21.
[120] EDPBI:DEBB:OSS:D:2019:53, https://edpb.europa.eu/decision-nr-53_en. A document regarded as 'final decision' is available here: https://edpb.europa.eu/sites/default/files/article-60-final-decisions/publishable_de_brandenburg_2019-10_right_of_access_decisionpublic.pdf. Due to opaque reasons, the EDPB has blanked out the name of the authority author of the decision.

following the request by the complainant to a company about information on his user account via a contact form. The company's customer service had responded via e-mail by asking the complainant to allow for the verification of his identity, by means of a redacted copy of his ID, which he was told would be used exclusively for the purpose of identity verification in connection with the requested data access. The complainant passed the verification process, but was informed that his user account had been suspended because there were indications that he had not yet reached the age of majority, and that was contrary to the company's general terms and conditions for the creation of user accounts. Moreover, the complainant was told that he would not be given access to their data unless he proved he had his parents' consent and submitted a '*birth certificate and a copy of your parents' identity card*'.

The complainant responded to the company that they were probably misinformed, as under Austrian law consent is legally binding with the completion of age 14, asked again for access to his personal data and warned the company he would otherwise lodge a complaint with the DPA, which he eventually did, focusing on the misuse of the information in his ID card. In its decision on the case, the relevant DPA decided not to decide on whether the request for parental consent and documents of the custodians constituted an infringement of the GDPR, in the sense of failing to facilitate the exercise of data subject rights. The authority argued that although there was clearly no reason for the company to request such information, the facts of the case proved that *'the complainant was very familiar with his rights'*, and that '*(a)t no time did he seem to be under the impression that he had to comply with the request*', so there was '*only a hypothetical risk that further data would be transmitted involuntarily'*.

The reasoning is astonishing, generally speaking, as it would imply that data controllers can request all sorts of unnecessary information of data subjects to the extent that data subjects are familiar enough with their rights to know such requests are completely unfounded, and that they can thus ignore them. More problematically, here the DPA paid no attention at all to the fact that the complainant was in any case a minor, in principle deserving special protection according to the GDPR. Not only was the complainant denied any special protection, but he was actually not even treated as a normal data subject deserving not to be requested unnecessary information, presumably because he knew too much to be treated as such. Such a *contextual invalidation* of vulnerability is certainly not what we propose. A recognition of the contextual nature of vulnerability must necessary be accompanied by a clear, strong protection of all data subjects, including the apparently less vulnerable.

6. Concluding remarks

This article calls for a twofold operation: reflecting on the implicit gender of the 'standard' data subject in data protection and privacy legislation, while opening a discussion on the benefits and drawbacks of a layered approach to data subjects' vulnerability, taking inspiration from feminist and gender studies.

Looking at how the notion of the data subject and the right to privacy and data protection have arisen in the Western legal tradition, we observed in Section 2 that although the 'data subject' was formally non-gendered, in many situations this notion implicitly referred to an 'average' (rational, circumspect, reasonable) individual silently envisaged as male, while female data subjects were seen as other, different than average, and needing privacy as a tool to balance their presumed inherent vulnerability. Looking at law and economics literature, we observed that consumer vulnerability is not univocally related to gender: although some 20th-century civil codes in Europe seem to refer to vulnerable female contractors, recent empirical studies show that being female might be a source of market vulnerability only in specific contexts.

As Section 3 argues, in modern data protection law, and especially in the GDPR, there is still limited light on the conceptual underpinnings of the notion of data subject, and also on the notion of vulnerable data subjects. Although in the text of the GDPR there is some room for interpretation to expand the protection of individual vulnerability, the only explicit example to vulnerability refers to children. The current implementation of the static 'group-based' vulnerability protection granted to them proves to be ineffective and useless, as data controllers massively moved to closing their eyes to the very existence of data related to children. When data protection authorities mention gender as source of vulnerability there is typically a problematic lack of discussion on the logic and consequences of such assumptions.

Section 4 calls for a wider reflection on vulnerability, moving beyond the idea that vulnerability has to be seen either as static and group-based (some people are vulnerable, because of the type of person they are), or as an inherent characteristic of humankind (everyone is vulnerable). A third way is layered vulnerability: vulnerability is here a contextual adjective in some social situations (some people have some vulnerabilities in some contexts). This layered approach seems in line with the GDPR risk-based approach (data protection risks are contextual and based on tangible adverse effects on individuals). This shift from static vulnerable or protected groups to contextual people 'with vulnerabilities' is somehow visible also in recent institutional documents in Europe, although inconsistently (Section 5). Resisting an essentialist conflation between the female and the vulnerable data subject is also important to maintain the notion of the 'mere' data subject as a duly inclusive.

Finally, it is crucial in any case to also retain from feminist thought a conception of vulnerability – and most generally of the very notion of 'protection' – as a double-edged sword, not necessarily always benefiting the holder of the label. In this sense, any refinement or development of the notion of vulnerability in data protection law should go

hand in hand with an explicit reflection of the consequences of such recognition – avoiding any risk of contextual invalidation, as Section 6 argues – so it represents real added value to their protection, instead of the opposite.