Universiteit
Leiden
The Netherlands

Assessing the (severity of) impacts on fundamental rights

Malgieri, G.; Santos, C.

Citation
Malgieri, G., & Santos, C. (2025). Assessing the (severity of) impacts on fundamental rights. *Computer Law And Security Review, 56*. doi:10.1016/j.clsr.2025.106113

Version:	Publisher's Version
License:	Creative Commons CC BY 4.0 license
Downloaded from:	https://hdl.handle.net/1887/4285926

Note: To cite this publication please use the final published version (if applicable).

Computer Law & Security Review 56 (2025) 106113

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

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

Assessing the (severity of) impacts on fundamental rights

Gianclaudio Malgieri [a,*], Cristiana Santos [b]

[a] Associate Professor of Law and Technology at Leiden University eLaw Center for Law and Digital Technologies, The Netherlands
[b] Assistant Professor of Law and Technology at School of Law, Utrecht University, The Netherlands

ARTICLE INFO

Keywords:
Fundamental rights impact assessment
AI Act
DSA
GDPR
Severity

ABSTRACT

"Risk to fundamental rights,", "impact on fundamental rights", "harm to fundamental rights" and "non-material damages" are all terms referring to similar problems, though inherently ambiguous and very problematic, especially in the age of AI-based technologies and digital platforms. Traditionally, legal and social sciences have two different approaches to analysing the impacts on fundamental rights: the rights-based approach and the risk of harm-based approach to fundamental rights. The rights-based approach is binary, focusing on whether rights and obligations are respected or violated. In contrast, a harm-based approach focuses on the anticipation of undesired events and measuring their likelihood and severity. However, focusing solely on "harms'' or "damages'' is reductionist, while existing impact assessment models often use vague terms like "gravity", "intensity," and "magnitude", which do not effectively help measure interferences with fundamental rights. Without operational criteria to measure these risks, most EU digital strategies demanding impact and risk assessments fail. Examples include the Data Protection Impact Assessment (DPIA) in the GDPR, Fundamental Rights Impact Assessments (FRIA) in the AI Act, and systemic risk assessments in the Digital Services Act (DSA). We posit that interferences with fundamental rights are seen as a spectrum that ranges from social contacts to violations, and these interferences can and should be measured. Thus, this article proposes a rights-based approach, combining it with elements from the harm approach and proposes an actionable parameter-based framework (also based on social meaning theories and social perception methodologies) to assess impacts on fundamental rights. The proposed multi-metric approach ensures a comprehensive assessment of the *severity* of impacts on fundamental rights within EU law, particularly in GDPR, DSA, and AI Act. This approach aims to inform policymaking, prioritise high-risk scenarios and propose mitigation measures in digital markets. This is especially important for detecting and addressing human vulnerabilities in interactions with digital technologies.

1. Introduction

The effective protection of fundamental rights is a growing challenge, especially in the age of AI and digital platforms. Human vulnerabilities are increasingly exposed to exploitation, and many new laws and regulations (especially in the EU) are introducing fundamental rights impact assessments alongside fundamental rights risk parameters to graduate safeguards to protect individuals. Our goal is to assess the impact on fundamental rights, recognizing the crucial need for comprehensive impact assessments as mandated by the GDPR, DSA, and AI Act.[1] We aim to operationalize transversal concepts, such as human vulnerability, from a fundamental rights perspective.

Accordingly, assessing impacts on fundamental rights and freedoms is essential to prioritise higher-risk scenarios and propose mitigation measures for digital markets, especially for detecting and mitigating situations of human vulnerability in the interaction with digital technologies (defined, indeed, as higher risks to fundamental rights).[2] The analysis and measurement of potential impacts of legal violations on fundamental rights has become an element of regulatory compliance in many pieces of both extant and incoming legislation requiring this

* Corresponding author.
E-mail address: g.malgieri@law.leidenuniv.nl (G. Malgieri).

[1] The risk-based nature of both the GDPR and AI act is beyond the scope of this paper. On the discussion of the role of the risk-based approach in both laws, see Raphaël Gellert, "The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?" *Journal of Ethics and Legal Technologies*, 3(2), 15-33, 2021. DOI: 10.14658/pupj-JELT-2021-2-2; Giovanni de Gregorio and Pietro Dunn, 'The European risk-based approaches: Connecting constitutional dots in the digital age' Common Market Law Review vol. 59(2) (2022) 473-500.

[2] Gianclaudio Malgieri, *Vulnerability and Data Protection Law,* Oxford University Press, 2023, passim.

https://doi.org/10.1016/j.clsr.2025.106113

Available online 28 February 2025
0267-3649/© 2025 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

precautionary approach strongly rooted in the positivistic risk paradigm wherein risks are presented as calculable and controllable constructs.[3]

Yet, the framing of risk seems an impossible challenge in the EU legal system, despite the explicit call to measure impacts on Fundamental Rights in many pieces of legislation. There is a foundational disagreement between business scholars affirming that anything can be quantified[4] and human rights scholars who are reluctant to quantifications of human rights or value.[5] While there are studies on *measuring the likelihood* of risks or providing risk assessment methodologies, very little research focuses on quantifying the *severity*[6] *of the impacts* of legal infringements on fundamental rights. This gap is not a coincidence, and it reflects the profound complexity of this topic; quantifying the severity of human rights impacts means understanding the real nature of what an impact on fundamental rights is, and this question is far from being answered.[7]

Without straightforward criteria to measure those risks to fundamental rights in practice (both at individual and collective levels), most of the EU digital strategies that demand assessment of impact and risks are meaningless. Eminent examples are the Data Protection Impact Assessment (DPIA)[8] and Data Protection by Design (DPbD) in the GDPR, Fundamental Rights Impact Assessments (FRIA) in the AI Act (together with other risk assessments duties in that regulation), or the systemic risk assessment in the Digital Services Act (DSA).

The legal term "risk to fundamental rights" (and, similarly, "risk to human rights" or even just "risk to rights") is inherently ambiguous. In law – and social sciences in general – we are used to counterposing a right-based approach *vis à vis* a risk of harm-based approach (or risk-based approach). The first is a yes-or-no approach, where rights and obligations are either respected or violated. A harm-based approach is a more gradual one, where the focus is not on strict legal situations (rights, obligations, violations) but on the anticipation of undesired (legal or factual) events and harm and the measurement of the likelihood and severity of their occurrence.[9] Both these approaches have some merits and some drawbacks, which we will explore in Section 2.

In this work, we embrace the right-based approach but aim to operationalize it by incorporating elements from the risk-based approach to make it applicable within the fundamental rights impact assessment framework, which became a milestone of EU digital laws. Interferences with fundamental rights are a spectrum (from mere social contacts to proper violations of fundamental rights). To measure the severity of interferences, however, focussing only on "harms" or "damages" is a very limited and reductionist approach. At the same time, many existing impact assessment models propose vague, circular, or self-referential terms (like "gravity", "intensity", "magnitude") which do not really help to operationalise the measurement of interferences with fundamental rights in concrete ways.

Thereafter, we propose a multi-metric approach to ensure the assessment of the severity of the impact on fundamental rights. Legislative and policy insights will draw our proxy approach: we discern how risks to legal violations are conceptualised within EU Law, in particular, in the GDPR, DSA, and AI Act, and we also collate evidence on the approaches to addressing risk convened by policymakers. Our typology of parameters is considered from an individual, collective, and societal perspective, allowing flexibility to cover the varied and evolving scope of risks and harms (proposed in Section 3).

Our analysis in this article further focuses on how to measure the severity of potential interferences with fundamental rights within an ex ante (before a violation occurs) and ex post evaluation (after a potential violation occurs). Ex ante assessments involve predicting and quantifying the potential severity of risks to fundamental rights before they manifest. This precautionary approach asks what the consequences might be if the risk materializes and requires developers and deployers to proactively mitigate those risks. Conversely, ex post evaluations occur after a potential violation, where courts determine whether the infringement of fundamental rights has occurred and, if so, whether it constitutes an actionable violation. In this phase, considerations often include whether necessary mitigating measures were in place, and whether an impact assessment had been properly conducted. By maintaining this distinction, we aim to contribute to both regulatory compliance (ex ante) and judicial remedies (ex post), ensuring a comprehensive approach to safeguarding fundamental rights in the digital era.

This article makes the following contributions:

- systematises and consolidates the literature on the harm and right-based approaches;
- disambiguates the concept of *risk* by distinguishing between violations and interferences to fundamental rights;
- considers that interferences to fundamental rights are a spectrum of different degrees that ranges from "social contacts" to violations, and these interferences can and should be measured;

[3] Allhoff F (2009) Risk, Precaution, and Emerging Technologies. Studies in Ethics, Law and Technology Volume 3, Issue 2 2009 Article 2, Risk_Precaution_Emerging_Technologies.pdf (allhoff.org).

[4] See Douglas W Hubbard, *How to Measure Anything. Finding the Value of Intangibles in Business*, Wiley, 2014.

[5] See, e.g., Sally Engle Merry, *The Seductions of Quantification, Measuring Human Rights, Gender Violence, and Sex Trafficking*, The University of Chicago Press, 2016.

[6] "Severity" means the magnitude of the risk or its impact if it materialises, CIPL https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf p. 26. It essentially depends on the prejudicial effect, or the level of consequences of the potential impacts. The gravity/seriousness of prejudice to a human right is usually assessed according to the following three elements: (i) its intensity, (ii) the consequences of the violation, and (iii) its duration, where the intensity of the violation is related to the importance of the violated protected legal interest. See also Altwicker-Hamori et al., 'Measuring Violations of Human Rights: An Empirical Analysis of Awards in Respect of Non-Pecuniary Damage Under the European Convention on Human Rights' (2016) 76 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV)/Heidelberg Journal of International Law (HJIL) 1-51; ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches Working Document, v1.0, December 2013.

[7] See, e.g., Karen Yeung and Lee A. Bygrave, "Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship". *Regulation & Governance*, 16: 137-155. https://doi.org/10.1111/rego.12401, 146.

[8] Recital 84, Article 24(1) and Article 35 GDPR. As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

[9] ''11/ The risk-based approach goes beyond a narrow "harm-based-approach" that concentrates only on damage and should take into consideration every potential as well as actual adverse effect, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust).'' Article 29 Data Protection Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', accessed 3 March 2024, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

- proposes a catalogue of operational parameters to assess *severity* of interferences with different fundamental rights from objective, subjective, individual, collective, and societal perspectives.

We claim that this parameter-based approach can inform policy-making and set benchmarks for assessing policy impacts, estimating impacts, and prioritising interventions.

2. The problems of current risk-based and harm-based approaches and the need for an operational approach

Contemporary approaches for assessing risks to fundamental rights typically fall into two distinct categories: risk-based approaches and right-based approaches.[10] We analyse these two approaches individually, highlighting both their limits and merits in the following sections. This analysis is necessary for building our new approach sought in section 3.

2.1. The origin of the risk-based approach

Regarding the origin of the risk-based approach to fundamental rights, it gained importance when the GDPR introduced the notion of "risks to the rights and freedoms of natural persons" precisely located in different Articles (e.g., 24, 25, 32, and 35) and, consequently, interpreters identified that Regulation (although implementing a fundamental right) as being risk-based.[11]

According to Van Dijk, Gellert, and Rommetveit, the introduction of data protection impact assessments (DPIAs) under the GDPR represents a shift from classical legal practices to more risk-based approaches. They argue that merging risks and rights in the manner proposed by the GDPR could unpredictably alter their meanings, thereby creating challenges in determining the actual "risk to a right".[12] Gellert acknowledges that the notion of "risk to a right" should be considered as risk of non-compliance with the GDPR principles.[13]

Some commentators of this "risk revolution" already identified the paradox of combining two concepts (risk and rights) that traditionally belong to different spheres of social fields and knowledge.[14] Risk and its management enable decision-making if risk is identified, analysed, evaluated and remedied in formal, systematic and rational processes, to anticipate and address consequences that might or might not occur in the future.[15] While risks[16] are inherently quantitative and probabilistic, rights tend to be qualitative, socially situated, and either violated or not.

Mantelero, acknowledging that fundamental rights impacts are often not based on measurable variables, relies on "the result of expert evaluation",[17] based on knowledge of case law, the literature, and the legal framework", leading to proxies of "range of risks" rather than precise measurements.[18] The reliance on experts' opinions is indisputably necessary but often theoretically problematic.[19] Nevertheless, although accepting that reliance, we – the writers and the readers, i.e. potential members of that group of "legal experts" – might agree that there is no solid and detailed guidance on how to assess those ranges of risks to fundamental rights. The goal of this article is indeed aimed at disentangling the opacity, vagueness, or circularity of some of the conceptual tools that usual impact assessment models adopt to measure interferences on fundamental rights.

Going back to the letter of the law, the most sophisticated (yet still ambiguous) explanation of the notion of risk to rights stems from recital 75 and Articles 24(1) and 25(1) of the GDPR. That recital describes risks as a composite result of the probability and severity of certain data processing activities, "which could lead to physical, material or non-material damage". Herein, the link between risks and rights seems to be "damages" - a private law concept referring to quantifiable losses to property, health, or other non-material "values".[20] On the other hand, even if the EU AI Act is considered to be a risk regulation,[21] it connects the concept of risks to the concept of "harm". Article 3(2) defines "risk" as the "combination of the probability of an occurrence of harm and the severity of that harm". Article 6(3) defines the scope of the "high-risk AI systems" and refers to "a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making". Article 7 also refers to "risk of harm" instead of "risk to rights". Interestingly, the rules about Fundamental Rights Impact Assessment refer more broadly to "impact on fundamental rights" (Article 27(1)).[22] Similarly, the right to explanation in the AI Act applies to the cases of "adverse impact on (...) health, safety or fundamental rights" (Article 86(2)). The Digital

[10] See the vivid academic debate on the point, Gellert, "We Have Always Managed Risks in Data Protection Law," 486; Macenaite, "The 'Riskification' of European Data Protection Law through a Two-Fold Shift," 517, 525; Claudia Quelle, "The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too", in *Data Protection and Privacy: The Age of Intelligent Machines*, ed. Ronald Leenes et al. (Hart Publishing, 2017). See also Bart van der Sloot, 'Editorial' (2017) 3 European Data Protection Law Review 1; See also the reply of Raphaël Gellert, 'On Risk, Balancing, and Data Protection: A Response to van Der Sloot' (2017) 2 EDPL 180; See also the counterarguments of Bart van der Sloot, 'Ten Questions about Balancing' (2017) 3 European Data Protection Law Review (EDPL) 187. Katerina Demetzou, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of "High Risk" in the General Data Protection Regulation' [2019] Computer Law & Security Review 105342.

[11] See, in general, Raphaël Gellert, *The Risk-Based Approach to Data Protection*, Oxford University Press, 2020.

[12] Van Dijk et al., A risk to a right? Beyond data protection risk assessments, CLSR, 2015.

[13] Raphael Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016) 2 Eur Data Prot L Rev 481.

[14] Niels van Dijk et al., 289.

[15] Dariusz Kloza, Thibaut D'hulst and Malik Aouadi, What could possibly go wrong? On risks to the rights and freedoms of natural persons in EU data protection law, their typologies and their identification, *Technology and Regulation*, 2024, p. 312, <https://doi.org/10.26116/techreg.2024.022>, ISSN: 2666-139X.

[16] International Organization for Standardization (ISO), ISO 31000:2018 defines risk management as an "effect of uncertainty on objectives" and expressed in terms of risk sources, potential events, their consequences, and their likelihood, – Guidelines, § 3.1 , <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>, accessed 2 February 2025.

[17] Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, Springer, 2022, 54.

[18] Idem.

[19] About the risks of relying on "science", see the provocative reflections in the Science and Technology Studies, e.g. Bruno Latour, *The Pasteurization of France followed by Irreductions*. Cambridge, MA: Harvard University Press, 1984 affirming that "science is politics by other means". See also Eve Seguin, Laurent-Olivier Lord; "Bruno Latour's *Science Is Politics By Other Means*: Between Politics and Ontology", *Perspectives on Science* 2023; 31 (1): 9–39.

[20] See Christian von Bar, Eric Clive, and Hans Schulte-Nölke. Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR). Outline Edition, Berlin, New York: Otto Schmidt, De Gruyter european law pub, 2009. https://doi.org/10.1515/9783866537279.

[21] Margot E Kaminski, 'The Developing Law of AI: A Turn to Risk Regulation' (2023) The Digital Social Contract: A Lawfare Paper Series 2 https://www.lawfaremedia.org/article/the-developing-law-of-ai-regulation-a-turn-to-risk-regulation accessed February 2025.

[22] Article 27(1)(c) also refers to "risk of harm likely to have an impact" on certain categories of people.

Services Act, in its rules about risk assessment, uses even different wording: "negative effects for the exercise of fundamental rights" (Article 34(1)(b)). In sum, we observe at least four parallel ways to mention very similar concepts: the GDPR refers to "risk to fundamental rights"; the AIA refers either to "risks of harm" or to "(adverse) impact on fundamental rights" and the DSA "refers to negative effects for the exercise" of those rights. Making sense of this chaos is one of the goals of this article.

2.2. The origin, merits and limits of the 'risk of harm' approach

The legal scholarship on the quantification of non-material damages goes back to the last decades and is largely situated on legal-political contexts and specific decisions of legislators.[23] However, limiting "fundamental rights impacts" to the legal concept of damage is clearly a very narrow approach, which does not take into account the nuances and complexity of the notion of fundamental rights.[24] To add more complexity to this scenario, however, recital 75 mentions some examples of these "risks to fundamental rights", e.g. "discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data … or any other significant economic or social disadvantage", but also "where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data", or when special categories of personal data are processed. This random miscellaneous of damages, including social or economic "disadvantages", violations ("discrimination"), rights "deprivations" and to mere sensitive activities (processing special categories of data), reveals the confusion of the legislator, or at least the awareness that there is no specific transversal definition of "risks to fundamental rights", delegating the understanding of the actual notion to courts and regulators. However, this particular confusion of recital 75 shows, in fact, a precious opportunity to go beyond a mere risk-of-damages approach.[25]

In sum, the risk-based approach (especially in the GDPR sense) has been generally interpreted narrowly as a risk of material or non-material damages to individuals. In other words, according to this interpretation, risks to rights exist when there is a likelihood of a negative event that will produce damage of a certain severity to individuals (data subjects or others). This approach considers risks to fundamental rights as a probabilistic analysis of (not neglectable) tangible harms, detectable facts, or quantifiable losses.

The *merit* of this approach is that it is more controllable and predictable than others. Interpreters can identify a list of possible individual "damages" as mentioned in laws or case law; we can determine the minimum level of damage severity (de minimis severity threshold)[26] that would legally matter (below that level of "loss'', we consider the event not producing real damage but mere nuisances), and we could anticipate the real-life negative events leading to those damages from a probabilistic perspective.

The *limits* of this approach are both theoretical and practical. Firstly, fundamental rights are not merely objects or assets but are moral boundary markers aimed at safeguarding human dignity.[27] Therefore, quantifying losses, even those that are non-material, fails to capture the full scope of harm in many scenarios, such as collective or community rights.[28] Secondly, the methodology for quantifying intangible damage is inherently flawed. The focus tends to be on sectors where numerical metrics are more straightforward, such as economic damages. By definition, economic damages are quantifiable, including losses like economic opportunities and chances (even indirectly, e.g. reputational harm). Outside the economic realm, the only other field where non-economic damages can be quantified effectively is medicine, wherein physical or psychological harm can be measured in terms of severity and probability.[29] However, this emphasis leads to a reductionist perspective.[30] It implies that violations of fundamental rights that do not result in economic, physical, or mental harm are not significant. Such a viewpoint limits the assessment to tangible harms and neglects broader, intangible impacts on fundamental rights, such as privacy or freedom of expression. These rights are inherently difficult to quantify and measure, complicating the establishment of a direct causal link between an action and its negative impact.

Ultimately, persisting with a risk assessment framework that views risks to rights merely from a business risk management perspective (i.e., the probability of an incident leading to some damage to individuals) results in three major issues:

1. Misunderstanding of the notion of fundamental rights, since this approach reduces fundamental rights to quantifiable metrics, ignoring their moral and dignity-oriented dimensions;
2. Ignoring many situations, in particular many scenarios where rights are collective or impacted in non-quantifiable ways;
3. Reducing the scope of analysis because it limits its reasoning to a few quantifiable metrics (mostly economic and health) and fails to

[23] See Draft Common Frame of Reference, Book VI, Chapter 2, Section 1, 101: "Meaning of legally relevant damage"; see especially Para. 4, "In this Book: (a) economic loss includes loss of income or profit, burdens incurred and a reduction in the value of property; (b) non-economic loss includes pain and suffering and impairment of the quality of life". See further Václav Janeček and Cristiana Santos, 'The Autonomous Concept of "Damage" According to the GDPR and Its Unfortunate Implications: Österreichische Post' (2024) 61(2) Common Market Law Review, p. 542. The authors note, while commenting the CJEU decision, that the more natural way of thinking about normative loss (qua interference with rights) would be to say that the rights are either interfered with or not. In effect, such rights-based thinking could therefore make it easier for the national courts to assess the intensity of the damage without reintroducing the threshold of seriousness.

[24] See, e.g., Gianclaudio Malgieri, *Vulnerability and Data Protection Law*, 172.

[25] Ibid., 171-175.

[26] However, the CJEU has affirmed that for what concerns the non-material damages in the GDPR, there is no "de-minimis threshold" that should be reached (see case C-200/23, Agentsia po vpisvaniyata v OL, 4 October 2024, par 149; see also the Case C-456/22 of 14 December 2023, *Gemeinde Ummendorf*, C-456/22, EU:C:2023:988, par. 17).

[27] Richard Dworkin, *Taking Rights Seriously*, Duckworth, London, 1977. See also Yeung and Bygrave, 143.

[28] See, for example, the AI Risk repository - a comprehensive database of risks from AI system, available online (https://airisk.mit.edu/#Repository-Overview). We observe an ambiguity between the different concepts used in this database (risks, harms, events), different targets or entities (end-users, systems, etc.) and it is absent a clear systematisation of parameters to qualify risks, Peter Slattery, Alexander K. Saeri, Emily A. C. Grundy, Jess Graham, Michael Noetel, Risto Uuk, James Dao, Soroush Pour, Stephen Casper, Neil Thompson, "The AI Risk Repository: A Comprehensive Meta-Review, Database, and Taxonomy of Risks From Artificial Intelligence." (2024), available at https://www.arxiv.org/abs/2408.12622.

[29] See, e.g., Hausman, Daniel. "The significance of 'severity'", *Journal of Medical Ethics* 45, no. 8 (2019), 545-551. See, also, Krischer, J. P. "Indexes of severity: conceptual development." *Health Services Research* 14, no. 1 (1979): 56.

[30] Ignacio Cofone, *The Privacy Fallacy*, CUP, 2024, 7.

consider the broader impacts on individuals' dignity and flourishing.[31]

Thus, a more comprehensive approach is needed to assess risks to fundamental rights in the digital ecosystem, one that transcends mere quantifiable metrics and encompasses the full spectrum of potential interferences.

2.3. The merits and limits of the rights-based approach

Right-based approaches primarily focus on direct violations of fundamental rights. In this light, Hildrebrandt[32] stresses the need to steer free from a risk or harm-based approach to fundamental rights.[33] Both Hildebrandt and Demetzou recall that the Court of Justice of the EU takes an approach based on the violation of rights instead of alternative approaches based on harm or damages.[34] This approach affirms that fundamental rights law aims to counter high violations for which "harm" is not a condition, and to establish a violation there is no need to prove harm. Only the violation of norms is at stake, whether that violation results in identifiable harm or not. Hildebrandt[35] further states that the consequences of norm violation are potential anomie, rather than harm. The author exemplifies her reasoning with the AI Act, which aims to prevent risks to health, safety, and fundamental rights and takes a risk approach. The rights-based approach to assessing risks to fundamental rights is solid and effective, particularly in avoiding a harm-reductionist perspective and taking fundamental rights seriously.

The great *merit* of this approach is to avoid any harm-reductionist approach, valuing the essence of fundamental rights as aimed at protecting human dignity in a broad sense. However, *limits* to this approach exist. The rights-based approach treats legal compliance in binary terms—rights are either upheld or violated, with no in-between. Further, significant challenges remain in operationalising this approach, considering the need to comply with all EU digital laws and the GDPR, especially regarding the assessment of the severity and likelihood of risks to fundamental rights. If a violation is a yes-or-no parameter, how can we *measure* the impact on fundamental rights according to the DPIA in the GDPR, according to the FRIA in the AI Act, or according to the systemic risk assessment in the DSA (all of which explicitly mention the likelihood and severity of risks)?[36]

Yeung and Bygrave propose a solution to make sense of the "right-based approach" in a legal framework with many indications to assess the "likelihood and severity" of impacts on fundamental rights.[37] They highlight the legal uncertainty in determining whether a situation constitutes a violation, especially in new contexts involving emerging technologies where the scope of violations might appear uncertain. We contend, however, that in many cases, the distinction between a violation and a non-violation is not clear-cut. If we could always wait for judicial clarification, the uncertainty would be resolved. But this is not practical. Therefore, the authors advocate for a precautionary approach, conceptualising the risk to fundamental rights as *normative uncertainty*.[38] Yet again, the *limit* of this approach is the lack of concrete parameters for detecting risks. The only guideline might be the normative proximity to "clear violations"—situations similar to those that are evidently violations. But what constitutes evidence, and who decides? Even seemingly clear-cut cases in court can have nuanced real-life implications. Furthermore, measuring this normative uncertainty in terms of likelihood and severity remains challenging.

2.4. What we must measure is the severity of "interferences" to fundamental rights

2.4.1. Violations vs interferences to fundamental rights

While the *violation* of fundamental rights may appear black and white, the *interference* with fundamental rights is not, as the CJEU confirmed.[39] Interferences are a *spectrum* of different degrees. Every interaction of humans with the surrounding environment and society can imply a certain form of interference with their fundamental rights, affecting their capabilities.[40] Depending on the context, the circumstances, and how the human values are translated in practice by the legislator (according to certain political sensitivities) and perceived by the individuals, by their group and community or by society at large, such interference can qualify from trivial (a mere "social contact") to a severe interference that a judge could consider a "violation" of fundamental rights.

The CJEU (see, e.g., *Digital Rights Ireland*,[41] *Google Spain*,[42] *Tele2*

[31] It is, however, interesting to notice that these quantifiable parameters have been recently loosened by the CJEU. The Court has affirmed that for what concerns the non-material damages in the GDPR, there is no "de-minimis threshold" that should be reached (see case C-200/23 , par 149; see also the Case C-456/22 of 14 December 2023, *Gemeinde Ummendorf*, C-456/22, EU:C:2023:988, par. 17). In addition, in the case C-200/23, Agentsia po vpisvaniyata v OL, 4 October 2024, par. 144, the Court affirmed that even the "*fear* experienced by a data subject with regard to a possible misuse of his or her personal data … is capable of constituting "non-material damage". Similarly, the court affirmed affirmed that the damage cannot be limited solely to damage of a certain degree of seriousness, in particular as regards the duration of the period during which the negative consequences of the infringement of that regulation were suffered by the data subjects (see Case C-200/23, par. 147).

[32] Mireille Hildebrandt, Talk on ''Beyond the GDPR'' on 22 September, https://www.cohubicol.com/assets/uploads/response-hildebrandt-purtova.pdf, slides 11-20.

[33] Katerina Demetzou, Risk to a Right under the GDPR - the risk of violation of the right to data protection: identification and assessment, PhD Thesis, Radboud University, 2025.

[34] Idem.

[35] Mireille Hildebrandt, Talk on ''Beyond the GDPR'' (n 29).

[36] See Article recital 75 of the GDPR interpreting Article 35. See also, Article 34 of the Digital Services Act, and Article 27 of the AI Act.

[37] Yeung and Bygrave, 146.

[38] See Yeung and Bygrave, 146. The authors do not name their approach as of "normative uncertainty", but this is how we interpret it.

[39] See ECJ, Case C-292/97, Karlsson and Others, ECLI:EU:C:2000:202, Judgement of 13 Apr. 2000, para. 45 "with regard to the aim pursued, disproportionate and unreasonable interference undermining the very substance of [a fundamental right]". See also Opinion of Advocate General Saugmandsgaard Øe at para. 82, Case C-207/16, Ministerio Fiscal (Oct. 2, 2018), http:// curia.europa.eu/juris/liste.jsf?num=C-207/16. referring to "a link between the seriousness of the interference found and the seriousness of the reason that could justify the interference". Digital Rights Ireland, Joined Cases 293 & 594/12 at para. 65; ECJ, Case C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:788, Judgement of 2 October 2018, para. 55

[40] The theory of interferences with fundamental rights or human rights and the human capability theori has been widely investigated in, e.g., Amartya Sen, Human Rights and Capabilities. *Journal of Human Development*, 6(2), 2005, 151–166. https://doi.org/10.1080/14649880500120491. See also, Martha C. Nussbaum, "Human Rights and Human Capabilities," *Harvard Human Rights Journal* 20 (2007): 23–24.

[41] CJEU, *Digital Rights Ireland*, ECLI:EU:C:2014:238, par. 60: "in view of the extent and seriousness of the interference with the fundamental rights".

[42] CJEU, 13 May 2014, Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, para 81: "In the light of the *potential seriousness of that interferenc*e, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing", emphasis added.

Sverige,[43] *Ministerio Fiscal*[44] and *La Quadrature du Net*[45]) constantly refers to the "*seriousness of interferences*'' with fundamental rights. The ECtHR, e.g. in the *Zakharov* case, referred to this same concept.[46] In other terms, both European Courts admitted that (even though violations can be a yes-or-no factor), interferences are a spectrum, where the severity ("seriousness") can be of varying degrees and so where the severity *can be measured*, as CJEU explicitly affirmed recently.[47] In sum, pursuant to assess the proportionality of human activities and fundamental rights, we need to be able to "measure the severity of interferences to fundamental rights", not only according to the proportionality principle in Article 52 of the EU Charter but also when secondary legislation obliges private entities to assess necessity and proportionality on fundamental rights, like Article 35(7)(b) GDPR.[48] In sum, as already affirmed by one of us, what we can and need to measure are the interferences to fundamental rights.[49]

We can make an example. Staring at someone in a crowd is perhaps a slight interference with their fundamental right to private life; filming someone in a crowd might be a more severe interference; filming someone in their living room (e.g. from an open window) is even more severe; and filming someone in their toilet is perhaps one of the most intense interferences with their private life.[50] Depending on the context (i.e. a) legislative (statutory or caselaw) indications; b) (individual, group, and social) sensitivity in that case; and c) consequences in one's life), some of these interference acts might be considered as a violation of fundamental rights. We might all agree that the toilet example is a clear violation, and probably most of us would agree that also filming someone in their living room is a violation, while the severity of interference caused by filming someone in a crowd is lighter and might be assessed on the basis of the circumstances, normative instructions, sensitivity perception, and consequences. Still, all of these interactions (even staring at someone) can be considered as more or less *severe* interferences with the fundamental rights of the surveilled individual.

As Yeung and Bygrave point out, fundamental rights are not tangible objects or natural phenomena.[51] They are based on human dignity, which cannot be simply categorised as violated or not. There are varying levels of flourishing.[52] If we adopt a merely black-and-white perspective (violation vs. non-violation), we perhaps reduce the discussion to a simplistic dichotomy, which lacks the nuance to account for the degrees of severity in the *interference* with dignity and human flourishing. Some interferences might be declared intolerable or inadmissible by a court and thus become recognised violations of fundamental rights. The goal of the next sections is to propose paramaters to measure these interferences. We clarify that these interferences do not necessarily equate to damage and that interferences encompass more than quantifiable economic or health losses.

2.4.2. The urgency and difficulty of measuring the "severity" of interferences

To measure these interferences effectively we need to identify appropriate parameters. The most common parameters used in impact assessment methodologies are severity and likelihood. Although most EU laws refer to risks as based on both severity and likelihood, our analysis will focus on severity rather than likelihood for two reasons: i) severity logically precedes likelihood because it helps determine the "what" (the misconducts, the events of interferences) and it informs the definitional core of the notion of interferences to fundamental rights; ii) once we determine severity, it is easier to quantify likelihood, because likelihood is based on more quantitative elements (probability science in mathematics) and the scholarship on likelihood seems already more precise and less vague.[53] Existing impact assessment methodologies offer numerous parameters, but they often fall short when it comes to measuring severity.

When impact assessment models refer to severity, these typically rely on vague concepts like intensity, gravity, seriousness, magnitude,[54] which are mere synonyms of severity and do not adequately explain how to assess the parameter of interference. In particular, Yeung and Bygrave identify three potential parameters: culpability, scale, and magnitude.[55] However, *culpability* is more relevant for determining sanctions than the severity of the interference. The severity of an interference does not

[43] CJEU, *Tele2 Sverige*, ECLI:EU:C:2016:970, par. 102: "Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure".

[44] CJEU, *Ministerio Fiscal*, ECLI:EU:C:2018:788, Judgement of 2 October 2018, para. 55: "the Court explained its interpretation by reference to the fact that the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question that that access entails".

[45] CJEU, 6 October 2020, C-511/18, C-512/18 and C-520/18 (*La Quadrature Du Net*), par. 131: "Specifically, it follows from the Court's case-law that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 *must be assessed by measuring the seriousness of the interference* entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness". Emphasis added.

[46] European Court of Human Rights, *Roman Zakharov v. Russia*, 2015, para. 232.

[47] CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net), par. 131.

[48] We are aware that the concept of (even private) entities conducting a fundamental rights balancing is controversial in the data protection scholarship. See e.g., Raphael Gellert, "We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection," *European Data Protection Law Review (EDPL)* 2 (2016): 481, 487 in favour of data controllers conducting balancing exercises and checking proportionality on fundamental rights. For the opposite view, see the critical response in Bart van der Sloot, 'Editorial' (2017) 3 European Data Protection Law Review 1. See also the reply of Raphaël Gellert, 'On Risk, Balancing, and Data Protection: A Response to van Der Sloot' (2017) 2 EDPL 180; See also the counterarguments of Bart van der Sloot, 'Ten Questions about Balancing' (2017) 3 European Data Protection Law Review (EDPL) 187.

[49] See Gianclaudio Malgieri, *Vulnerability and Data Protection Law*, 167, footnote 2: [when analysing impacts on fundamental rights] "the concept of interference is more appropriate than the term harm because not all interferences with fundamental rights can lead to quantifiable harm. Analogously, *the concept of interference is more appropriate than "violation": the first is a gradual notion, while the latter is a yes-or-no notion.* For the purpose of this book, when I address the concept of risk, I prefer to use a neutral and gradual notion of interference with fundamental rights and freedoms". Emphasis added.

[50] See, e.g., Bert-Jaap Koops et al., "A Typology of Privacy", University of Pennsylvania Journal of International Law 38(2): 483-575 (2017).

[51] Yeung and Bygrave, 143.

[52] See John Kleinig and Nicholas G. Evans, "Human Flourishing, human dignity and human rights," *Law and Philosophy* 32, no. 5 (2013): 539–64. http://www.jstor.org/stable/24572414.

[53] For an overview see, e.g., Alessandro Mantelero, *Beyond Data*, 55. See also Gianclaudio Malgieri, *Vulnerability and Data Protection Law*, 2023, 176-177.

[54] See, e.g., ENISA, Guidelines for SMEs on the security of personal data processing, December 2016, 14. See also ISO 31000:2018(en), Risk management - Guidelines, referring to "nature and magnitude of consequences". See, also, Alessandro Mantelero, *Beyond Data*, 57 referring to "gravity" of impact. See, the Dutch Fundamental Rights Impact Assessment,75, referring to "seriousness" of impact.

[55] See Yeung and Bygrave, 146: "(...) "culpability (e.g. particularly "egregious" moral wrongs, in which intentional violations are more culpable than unintentional violations), scale (i.e. whether only a few individuals are affected as opposed to whole populations), and magnitude (e.g. reading only one personal letter without permission in contrast to reading 5 years' worth of personal diaries)", Yeung and Bygrave, 146.

increase based on the violator's intentions or their psychological status. The *scale* parameter is interesting, even though just limited to the quantification of the number of people affected. The *magnitude* parameter is often tautological and fails to provide clear, actionable criteria. On the other hand, Mantelero[56] asserts that the severity of the expected consequences is based on two variables: i) gravity, and ii) effort to overcome it and to reverse adverse effects. He further claims that the assessment of gravity typically involves three key elements: i) intensity, ii) consequences of the violation, and iii) duration. These elements are important, but not further operationalized and might need better systematisation.

In this article, we propose a comprehensive list of non-exclusive, non-exhaustive, but relevant parameters to measure interferences, aiming to avoid reductionism or a sole focus on harm. These parameters are potentially the basis of a new interdisciplinary methodology for assessing (the severity of) risks to fundamental rights since they combine different dimensions and approaches (from legal hermeneutics to social and psychological sciences).

3. Measuring interferences. a catalogue of parameters

Our approach aims to overcome the limitations of both risk-of-harm-based and right-based methodologies. We do accept the right-based approach, but to make it more operational, we would focus on the severity of "interferences" rather than on "violations."[57]

Reflecting on the core values underlying fundamental rights, i.e., the dignity principle justified by the flourishing of individuals, the severity of interference should be determined based on the core meaning of each fundamental right that might be affected.[58] We should analyse how the "content" of fundamental rights is interfered with and how severely.[59] For instance, privacy rights encompass values such as personal autonomy, human dignity,[60] physical and mental integrity, and identity. Similarly, freedom rights involve personal autonomy, pluralism, and democracy. The full realisation of these values serves as the benchmark for assessing interferences of external activities on these rights and freedoms.[61] Simply put, we consider that risks (of meaningful interferences) to fundamental rights occur when certain practices might compromise the dignity and the flourishing of individuals.

3.1. Methodological foundations for assessing the severity of infringements to fundamental rights

The following outlines our methodological approach for assessing the severity of infringements to fundamental rights.

3.1.1. Alignment of concepts for impact assessment

In this article, we decide to use the following terms that provide clarity and legal certainty to any impact assessment:

1. *Infringement* of rules that safeguard fundamental right; given the relative, transient, contextual and political nature of the notion of dignity and flourishing,[62] we position a risk to a fundamental right within a normative lens. The law delineates how dignity and flourishing are achieved through specific rules and regulations that safeguard fundamental rights. Accordingly, we assert that risks to fundamental rights are present when there is a potential *infringement* of clear, positive rules established by laws or jurisprudence, *i.e.*, non-compliance with some secondary legislation rules (provisions in directives, regulations, etc.) or with some rules set by the Courts when interpreting fundamental rights;
2. *Violations* of fundamental rights, as discussed in section 2.4;
3. *Interference* with fundamental rights; we refer to interference as a spectrum that goes from no significant effects on fundamental rights to proper violations (point 2 above). To measure interferences, we first look at infringements (point 1 above) of positive legal rules implementing fundamental rights.
4. *Damages, harms, adverse effects* used in different contexts and refer to more quantifiable negative outcomes (e.g. physical, mental, economic) of an event or a situation (see section 3.4).

3.1.2. Three-tiered assessment of severity to fundamental rights

To avoid a strong dichotomy between rights-based and risk-based approach,[63] we introduce three-tiered assessment composed of three-high level parameters[64] to measure the severity of rights infringements: objective, subjective, and real-life consequences of those violations:

1. The *objective normative evaluation of the severity* of an infringement, as sometimes identified by the laws themselves (if this is the case) or considering the cumulation of rules/principles violated, the duration, scope and the reversibility of the infringement (Section 3.2);
2. The *social* and *inter-subjective meaning of the severity* of this infringement, i.e. how severe is considered the infringement by the society at large, by specific groups and by individuals (Section 3.3);
3. The real life tangible *consequences of this infringement on the lives* of the individuals affected or of their group or society, analysed in terms of money, scale, well-being, and reversibility. Tangible impacts matter, but not (only) as losses or damages, since we consider a broad range of consequences in terms of changes in life circumstances (Section 3.4)

From an *objective lens*, we consider objective parameters based on both quantitative factors (such as duration and scope of infringements) and qualitative factors (including normative provisions in the law, irreversibility, and impacts on multiple fundamental rights). These parameters are conducive to assessing the severity of the impacts of fundamental rights violations. Since these parameters rely on legal provisions, their focus is on the "infringement" of rules that safeguard fundamental rights.

A complementary way to assess the severity of a legal infringement of fundamental rights involves considering the *social meaning* or *the inter-*

[56] Alessandro Mantelero, The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template, Computer Law & Security Review 2024 (forthcoming), p. 22.

[57] About the different uses and meanings of the term "*violations*", "*infringement*" and "*interference*" in this paper, see Section 2.3 above.

[58] Dutch Ministry of Interior and Kingdom Relations, Impact Assessment Fundamental rights and Algorithms, March 2022, https://www.government.nl/documents/reports/2022/03/31/impact-assessment-fundamental-rights-and-algorithms, p. 75.

[59] Koen Lenaerts, Limits on Limitations: The Essence of Fundamental Rights in the EU. *German Law Journal*. 2019; 20(6):779-793. doi:10.1017/glj.2019.62.

[60] Human dignity is correlated to the right to personality and the right to information self-determination in the context of data processing in the Guiding principles on the judgement of the First Senate of 15 December 1983, Judgement of 15 December 1983 - 1 BvR 209/83, paragraphs 146-148.

[61] Dutch Ministry of Interior and Kingdom Relations, Impact Assessment Fundamental rights and Algorithms, p. 75.

[62] John Kleinig and Nicholas G. Evans. "HUMAN FLOURISHING, HUMAN DIGNITY, AND HUMAN RIGHTS." *Law and Philosophy* 32, no. 5 (2013): 539–64. http://www.jstor.org/stable/24572414.

[63] Article 29 Data Protection Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', accessed 3 March 2024, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf: "…the Working Party is concerned that both in relation to discussions on the new EU legal framework for data protection and more widely, the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles, rather than as a scalable and proportionate approach to compliance. The purpose of this statement is to set the record straight."

[64] We use criteria or parameters interchangeably.

subjective understanding of such an infringement. As posed by the European Court of Human Rights (ECtHR), the severity of a violation should be assessed not only by what is objectively at stake in a particular case but also by taking into account the applicant's subjective perception.[65] A reference to the subjective perception of interferences with one's fundamental rights is also emerging in the AI Act (e.g., Article 86). Subjectivity can be analysed from three different perception levels: the individual level, the group level, and the societal level. These three levels are often mentioned in risk management methodologies.[66] The emphasis that we give on perception collection is not only driven by the wording of the case law of the European courts but also based on the new awareness that legal scholars are giving to the notion of empathy[67] and emotional trustworthiness[68] in the field of law and public administration.[69] In addition, this emphasis on bottom-up perceptions, group experiences, and subjectivity can also be a way to take into account the relevant feminist, post-colonial, and queer critiques of the traditional top-down and privileged-conformant interpretations of fundamental rights and legal principles.[70]

Lastly, we can assess the impact of a legal infringement on a fundamental right, considering parameters that capture the resulting *adverse effects in one's life*.

3.1.3. Ex ante approach

In this article, we primarily focus on an *ex ante* approach for assessing potential impacts on fundamental rights, particularly in the context of emerging AI and digital technologies. Our analysis centers on how to measure and evaluate the severity of potential interferences with these rights *before* a violation occurs. This preventive approach aligns with the requirement for technology developers and deployers to conduct impact assessments, such as those mandated by Article 35 of the GDPR, Article 34 of the DSA, and Article 27 of the AI Act. These assessments aim to identify and mitigate risks to prevent violations from materialising. Companies will need to apply appropriate and rigorous impact assessments if they do not want to incur in violations and sanctions either under the GDPR[71] or under the DSA[72] and AI Act.[73] Adopting our suggested framework for assessing the severity of fundamental rights infringements can facilitate compliance.

However, we acknowledge that our reflections also apply to *ex post* scenarios, where courts evaluate actual violations of fundamental rights. In ex post cases, the focus shifts from assessing potential risks to determining whether a violation has occurred and, if so, whether it can be justified or balanced against other rights. Moreover, the presence of precautionary measures, such as impact assessments, becomes relevant in ex post evaluations, as courts may consider whether these were properly conducted and adhered to before the alleged violation occurred. Thus, while our primary focus is on ex ante impact assessments, we believe that understanding how to measure the severity of interferences with fundamental rights is essential in both phases.

3.1.4. Parameter interconnection

In this analysis, we favour parameters that are common to various and different fundamental rights and are not specific to any particular right (e.g., the categories of personal data affected by an infringement only regard the fundamental rights to data protection and privacy). This approach ensures that the model can be applied horizontally across different types of rights.

Our aim is not to identify a fully comprehensive list of parameters for all fundamental rights. That may, in fact, be next to impossible, given the nature and the scope of such rights and the diversity of contexts to which they could potentially be applied.

The proposed high-level parameters are indicative-approximate, cumulative and additive, enabling a qualitative risk classification for each parameter as low, medium, or high. Our comprehensive approach allows for a more holistic evaluation of interferences, better-guiding policymaking and enhancing the protection of fundamental rights in a rapidly changing digital landscape. Determining the severity of a legal violation is not a straightforward mathematical calculation where individual factors are considered in isolation. Instead, it involves a comprehensive assessment of the specific circumstances of the case, with all factors interconnected. Therefore, in reviewing the seriousness of the interferences on a fundamental right, regard should be given to the interference as a whole. Any quantification must always be based on a human assessment of all relevant circumstances of the case. Considering the legally, politically, socially, and culturally situated nature of human dignity and fundamental rights, we rely on different parameters implementing the essence of those rights in practice and in specific contexts. As the dimension of severity is contextual and needs to be 'measured', it is important to identify the key qualitative[74] parameters to be used for this purpose. Concerning the *nature* of the proposed severity parameters, we identify severity parameters that pertain to legal violations but are not related to sanctions; accordingly, the intentional or negligent nature[75] of the infringement is relevant only for determining the fine and not for our primary model.

[65] ECHR Practical Guide on Admissibility Criteria, Updated on 31 August 2023, p. 83 https://www.echr.coe.int/documents/d/echr/admissibility_guide_eng

[66] As put by CPL in its ''Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU'', the framework for identifying covered high-risk AI applications should involve the use of impact assessments designed to assess the likelihood, severity and scale of the impact of the AI use. Such impact assessments would include the following considerations: severity and likelihood of harm to individuals, groups, or society at large (relying on conclusions that can be reached with reasonable certainty), p. 2, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_risk-based_approach_to_regulating_ai_22_march_2021_.pdf

[67] Patricia Mindus, "When is lack of emotion a problem for justice? Four views on legal decision makers' emotive life", *Critical Review of International Social and Political Philosophy*, 26(1), 2021, 88–103. https://doi.org/10.1080/13698230.2021.1893254. Malou Beck and Sofia Ranchordas, "Empathy as a Public Value: overcoming administrative vulnerability and rehumanizing (digital) government", in Goossens, J, Keymolen, E, Stanojević, A (Eds.); *Public Governance and Emerging Technologies: Values, Trust and Compliance by Design* (Springer 2025, forthcoming), Available at SSRN: https://ssrn.com/abstract=4910290. See also Chalen Westaby, & Emma Jones, "Empathy: an essential element of legal practice or 'never the twain shall meet'?" International Journal of the Legal Profession, 25(1), 2017, 107–124. https://doi.org/10.1080/09695958.2017.1359615

[68] See, e.g., Chris Reed, *AI Fairness and Beyond*, Hart, 2024, 194.

[69] Sofia Ranchordas, "Empathy in the Digital Administrative State", 71 Duke L.J. 1341-1389 (2022), Available at: https://scholarship.law.duke.edu/dlj/vol71/iss6/4

[70] See, e.g., Vaditya, V. (2018). Social Domination and Epistemic Marginalisation: towards Methodology of the Oppressed. *Social Epistemology, 32*(4), 272–285. See also Houh, E. M. S., & Kalsem, K. (2015). Theorizing Legal Participatory Action Research: Critical Race/Feminism and Participatory Action Research. *Qualitative Inquiry, 21*(3), 262-276; Anna Grear, *Redirecting Human Rights, Facing the challgnes of corporate legal humanity,* Springer Nature Link, 2010.

[71] For example, in 2024, the Danish Data Protection Authority fined a company due to the absence of an impact assessment https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/netcompany-indstilles-til-boede, accessed February 2024.

[72] See Articles 73 and 74 of the Digital Services Act.

[73] See Articles 99 about the duty of Member States to lay down the rules on penalties for the violations of the AI Act provisions.

[74] Qualitative parameters do not use numbers to express impact but instead use rating scales to describe impact of risk, such as low, medium and high risk.

[75] For example, as per art. 83(2)(b) of the GDPR.

3.1.5. Anchoring on impact assessment methodologies

Developing a parameters-based approach to measuring the severity of fundamental rights interferences required an in-depth literature review including policy reports[76] and methodological frameworks[77] on fundamental rights impact and risk assessments, and legal scholarly analysis of EU case-law, EU laws requiring risk assessments to fundamental risks, and legal scholarly works. The identified parameters are either derived from legal or policy provisions – cited were appropriated to confer their authority basis–, or substantiated through the author's analytical reasoning.

3.2. Objective parameters to assess the severity of legal infringements

As already explained, we adopt a "risk of violation" approach as a starting point, but we develop it through different interference measurement parameters. Our parameters in this Section focus on objective positivist factors, i.e., how the legislator decided to interpret, implement, and substantiate a specific fundamental rights (e.g., through secondary legislations, statutes, regulations, acts). An analogous consideration applies to judges interpreting the letter and the spirit of the law.

This first element that we assess whether an interference is serious (i.e. pending towards a proper violation) is the existence of an infringement of some more or less specific rules that implement fundamental rights in practice. As an example, to understand if there is a violation of the fundamental right to data protection (Art. 8 EU Charter) we first consider if there is an infringement of one of the provisions of secondary legislation implementing it, i.e. the GDPR. At the same time, we should consider the specific rules emerging from the case law of the CJEU and ECtHR. Another example, in relation to the right to non-discrimination (Art. 21 EU Charter), could be assessing if there is any infringement of EU anti-discrimination directive and regulations. We recognise that the link between fundamental rights and secondary legislation (or case law) is not always straightforward. However, we reaffirm that the parameters outlined in this article are contextual and non-exhaustive.

Table 1 mentions the parameters we consider relevant for objectively assessing the severity of an infringement, in particular, normative instructions on severity provided by the law (e.g., prioritising the severity of certain violations over others), reversibility of an infringement, its duration, and its scope.

Table 1
Objective parameters and sub-parameters to assess the severity of a legal infringement.

Objective parameters to assess the severity of infringement of laws (implementing one or more Fundamental Rights)	Sub-parameters
Normative instructions	the law can establish internal criteria to assess the severity of a legal infringement, giving a severity priority to certain violations above others the law can establish fiduciary duties of care the law can determine fines according to the seriousness of the violation
Reversibility of the the infringement	reversibility
Duration of the infringement	long duration frequency
Scope of the infringement	geographical scope; potential number of people and cases in abstract terms
Simultaneous multiple infringements	legal violation potentially infringing one or different other laws

3.2.1. Normative instructions of severity

Once a specific infringement of provisions (from laws or caselaw which directly implement fundamental rights) is identified, we should determine its degree of severity, since not all infringements are equally serious. The primary parameter for measuring severity is often the law itself (what we refer to as normative instructions of severity). In many cases, it is the law that establishes a hierarchy of infringement seriousness. Below we offer examples of EU laws whose protective purpose safeguards a fundamental right, which also confer criteria to assess the severity of a legal infringement.

i) The law can establish internal criteria to assess the severity of a legal infringement

For example, Article 83 (2) of the GDPR explicitly refers to the seriousness of the infringement. It includes: a) ''the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them (paragraph a); b) the intentional or negligent character of the infringement (paragraph b); or c) the categories of personal data affected by the infringement (paragraph g).[78]

At times, Courts might establish a hierarchy among different fundamental rights. For example, the ECtHR referred to the right to life (Article 2) and the prohibition of torture (Article 3) as the "most fundamental provisions" in the Convention, and as "enshrining one of the basic values of the democratic societies making up the Council of Europe".[79] Any violation of these rights is therefore likely be considered

[76] United Nations Human Rights Office of the High Commissioner, ''UNHR's Guiding Principles on Business and Human Rights, 2011; Danish Institute for Human Rights, ''Guidance on Human rights impact assessment of digital activities'', 2020; Access Now and ECNL, ''Towards Meaningful Fundamental Rights Impact Assessment under the DSA'',2020; European Union Agency for Fundamental Rights, ''Getting the future right: Artificial intelligence and fundamental rights, 2020; OECD, ''Measuring Consumer Detriment and the Impact of Consumer Policy Feasibility study'', DSTI/CP(2019)13/FINAL, 2019; Government of the Netherlands, Fundamental Rights and Algorithmic Impact Assessment, 2021.

[77] Council of Europe, Methodology for the Risk and Impact assessment of Artificial Intelligence Systems from the point of view of Human Rights, Democracy and the Rule of Law (HUDERIA methodology), CAI(2024)16rev2; Catalan Data Protection Authority, ''FRIA model: Guide and use cases FRIA methodology for AI design and development'', 2025; French Data Protection Authority (CNIL), ''Privacy Impact Assessment (PIA) Methodology'', 2018; National Institute of Standards and Technology (NIST), ''The Assessing Risks and Impacts of AI (ARIA) Program Evaluation Design Document'', 2024; Vanja Skoric, Giovanni Sileno, and Sennay Ghebreab, 'Critical Criteria for AI Impact Assessment' (2024) 1(3) *Journal of AI Law and Regulation* 281.

[78] ''(...) *7/ Risks, which are related to potential negative impact on the data subject's rights, freedoms and interests, should be determined taking into consideration specific objective criteria such as the nature of personal data (e.g. sensitive or not), the category of data subject (e.g. minor or not), the number of data subjects affected, and the purpose of the processing. The severity and the likelihood of the impacts on rights and freedoms of the data subject constitute elements to take into consideration to evaluate the risks for individual's privacy*'', p.4, Article 29 Working Party (WP 208) ''Statement on the role of a risk-based approach in data protection legal frameworks'', Adopted on 30 May 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[79] ''*The Court considers that, (...) the right under Article 1 of Protocol No. 13 not to be subjected to the death penalty, which admits of no derogation and applies in all circumstances, ranks along with the rights in Articles 2 and 3 as a fundamental right, enshrining one of the basic values of the democratic societies making up the Council of Europe*'', Case Al-Saadoon and Mufdhi v. UK, Judgement No. 61498/08 (Eur. Ct. H.R. March 2, 2010), para 118.

"serious".[80] Moreover, the fact that certains rights are non-derogable (even in national emergency situations (Article 15)), or do not allow for exceptions, such as the prohibition of torture (Article 3) and the prohibition of slavery or servitude (Article 4(1)), indicates their particular importance within the Convention.

Limitations of the parameter

The Convention itself does not explicitly establish a hierarchy of rights. For example, it can hardly be maintained that the prohibition of discrimination (Article 14), mentioned last in the section on rights, is the least important of the Convention rights. It should be noted that not all legislation pertaining to fundamental rights includes a scale of severity of a legal violation similar to that found in the GDPR. This is because not all laws encompass secondary law protecting a fundamental right.

ii) The law can establish fiduciary duties of care

A supervisory authority may attribute more weight to the assessment of severity when there is a clear imbalance between the involved parties, particularly if an explicit or implicit fiduciary duty of care has been violated. This is the case when an individual is an employee, pupil, or patient, or where the infringement occurs within a university, public administration, border control, or involving vulnerable data subjects, in particular, children,[81] or individuals based on characteristics protected under EU non-discrimination law, i.e. the open-ended list of grounds prescribed in Article 21 of the EU Charter. A similar reference to fiduciary duties of care as a benchmark for assessing the severity of interferences can be found in the Unfair Commercial Practices Directive, where the violation of the trader's "professional diligence" is one of the two conditions for considering a commercial practice as "unfair".[82]

Limitations of the parameter

Challenges in defining and enforcing such duties can span across contexts and sectors, and it is also dependable on jurisprudential interpretations and more rigorous legal frameworks with respect to vulnerable parties.

iii) The law can determine fines according to the seriousness of the infringement

The more serious the infringement, the higher the fine is likely to be.[83] This is the case, for example, with Article 83 (4) (5) of the GDPR. For instance, an infringement concerning obligations on controller/processor and certifications, as outlined in paragraph 4, will be subject to fines up to 10.000.000 EUR. Conversely, infringements related to basic principles for processing, data subjects' rights, and transfers of personal data to a third country are bound to higher fines of up to 20 000 000 EUR (paragraph 5).

Limits of this parameter

The link between fundamental rights and secondary legislation (or case law) is not always clear, and many laws do not establish a hierarchy of infringement severity. In addition, as affirmed above, the sanction parameters that the secondary law sometimes uses for different violations do not always reflect the severity scale of a violation, but it might include other external considerations, like culpability, specific deterrence goals, and other utilitarian policy reasons of the legislators. However, we reaffirm that the parameters in this article are contextual, proxy-based, operational and non-exhaustive.

3.2.2. Reversibility of the infringement

The objective reversibility of an infringement can be considered to evaluate the severity of an infringement in abstract terms, independent of its impacts on individuals. The (ir)reversible nature of the infringement clearly influences its severity.

For example, making a discriminatory decision when hiring an LGBT+ person might constitute an irreversible infringement of Directive 2000/78/EC – as a direct implementation of the fundamental right of non-discrimination as enshrined in Article 21 of the Charter – regardless of the nature or reversibility of the measurable consequences for individuals. At the same time, if providers of digital intermediary services have a delay in complying with the transparency requirements of Article 15 of the Digital Services Act (which might be seen as an interference with the fundamental rights of freedom of speech and expression), such an infringement would not be irreversible. Yet on the other hand, infringing laws related to asylum requests by denying migrants entry into European countries is more irreversible than the case of a company that forgets to keep a record of its data processing activities, as per Article 30 of the GDPR, though it does it promptly after the regulatory authority so requests.

Limitations of the parameter

The reversibility parameter will mostly depend on the type of violation and on where there is a specific secondary law (or a clear set of rules emanating from the case law of the European Courts) that implements a fundamental right. In addition, we consider this parameter as an objective, abstract parameter of the severity of an infringement; however, the boundary between this parameter and the real consequences on individuals (e.g. harms, damages, adverse effects) is not always clear-cut. The irreversibility of some infringements might depend on the irreversibility of some consequences and vice versa. Reversibility of impacts related to an infringement is examined in section 3.4.

3.2.3. Duration of the infringement

The duration of the infringement, and thus, the duration of the restriction to the rights,[84] is explicitly referred to in legislation.[85] The duration assessment factor considers the length of time over which the violations occurred. A regulator may generally attribute more weight to

[80] Altwicker-Hamori, Szilvia and Altwicker, Tilmann and Peters, Anne, Measuring Violations of Human Rights: An Empirical Analysis of Awards in Respect of Non-Pecuniary Damage Under the European Convention on Human Rights (July 16, 2015). Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV)/Heidelberg Journal of International Law (HJIL) 76 (2016), p. 18.

[81] EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR Version 2.1 Adopted on 24 May 2023 p.18, https://www.edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf.

[82] See Article 5(2)(a) of the Directive 2005/29/EC (Unfair Commercial Practices Directive).

[83] Parag 49. *Almost all of the obligations of the controllers and processors according to the Regulation are categorised according to their nature in the provisions of Article 83(4)–(6) GDPR. 21 The GDPR provides for two categories of infringements: infringements punishable under Article 83(4) GDPR on the one hand, and infringements punishable under Article 83(5) and (6) GDPR on the other. The first category of infringements is punishable by a fine maximum of €10 million or 2% of the undertaking's annual turnover, whichever is higher, whereas the second is punishable by a fine maximum of €20 million or 4% of the undertaking's annual turnover, whichever is higher. Parag 50. With this distinction, the legislator provided a first indication of the seriousness of the infringement in an abstract sense. The more serious the infringement, the higher the fine is likely to be.* EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR Version 2.1 Adopted on 24 May 2023, https://www.edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf.

[84] Heleen Janssen, Michelle Seng Ah Lee, Jatinder Singh, Practical fundamental rights impact assessments, International Journal of Law and Information Technology, 2022, 30, 200–232 https://doi.org/10.1093/ijlit/eaac018, p. 217.

[85] Article 83(2)(a) GDPR.

an infringement that has a longer duration persisting over an extended period of time (or does not cease to terminate),[86] than to violations that occur for only a brief period of time. In particular, the duration can be considered in different facets to assess the severity of an infringement:

i) Long duration

An infringement that occurs over a lengthy period of time or temporarily. For example, an extended unlawful deprivation of liberty;[87]

ii) Frequency

An infringement that is repeated or recurring over a period and thus reveals a consistent pattern of violations; or different types of similar violations occurring within the same contexts, e.g. violation of the same legal provision that vary in terms of practices, contexts, or parties involved, which recur over time.

To illustrate, consider a person subjected to persistent cyberbullying on a social media platform over several months, involving hateful messages and defamatory posts targeting her personal life, appearance, and character. Despite reporting the abuse, this platform fails to remove the harmful content. The failure of the platform to address the harassment, despite reports, indicates the frequency of the infringement of the fundamental right of human dignity and a problem with the platform's content moderation policies.

Limitations of the parameter

The duration of an infringement needs to be considered within a context, including factors such as the number of people, the type of infringement. It cannot be quantified in silos, making it more complex to measure the parameter itself. Additionally, not all serious violations are of extended duration. In some cases, the duration of the violation might not always be stated in the judgement, or reported in a complaint, and thus, can be hard to determine with certainty.

3.2.4. Scope of the infringement

The scope, or pervasiveness parameter[88] assesses the extent of the violation(s) by considering:

i) the potential number of people (involved, not necessarily affected);[89]
ii) number of infringement cases; and/or
iii) geographical or demographic widespread of the violation.

The geographic scope requires determining whether it is local, national, or cross-border. Consider the scenario of a misinformation campaign spreading rapidly across various social media platforms, reaching millions of users worldwide regarding the (in)effectiveness of vaccines or the spread of infectious diseases, impacting such users and leading to confusion, fear, and potentially harmful conduct. Despite efforts by fact-checkers to debunk the root of misinformation, it continues to be disseminated due to the platform's algorithms and user engagement dynamics. The geographic widespread dissemination of misinformation highlights the significance of this parameter in evaluating the impact of fundamental rights violations (right to freedom of expression and access to accurate information) beyond borders.

This parameter is objective, considered in abstract terms, focusing solely on the extent of the violation, without accounting the effects or impacts on those affected, which is discussed under "Adverse effects" in section 3.4. Consider the example of a small company with 50 employees with a hiring policy discriminating against female candidates for certain positions, resulting in fewer women being hired compared to men. The scope of the violation refers to the absolute number of employees affected by the policy (if the policy affects 20% of the workforce, that would mean approximately 10 employees), without further considerations on whether, how, or when any of the concrete candidates had adverse effects (e.g., economic effects, psychological effects, etc.) as a consequence of that policy.

Limitations of the parameter

This parameter provides quantitative results and it is mostly actionable where it is possible to discern the absolute number of persons within smaller or well-boundary organisations or contexts. However, it is not always applicable, since it is not always easy to determine the scope of an infringement as an independent parameter, i.e. not related to the scale of the consequences, effects, damages (see Section 3.4).

3.2.5. Simultaneous multiple infringements

The seriousness of an infringement can be determined by the fact that one legal violation can be subsumed not only to several legal provisions of one concrete law,[90] but potentially infringing different other laws protecting fundamental rights, thereby confirming that the more numerous the violations, the more severe is the infringement. Consider the case of a company using sensitive data on race without the explicit consent of users for the purpose of online behavioural advertising. Such practice contributes to simultaneous infringements of Articles 6, 9, 22 of the GDPR and 26(3) of the DSA.

Limitations of the parameter

Sometimes the apparent simultaneous infringement of multiple provisions might be a mere formalistic requirement, especially when the law states the same obligation or prohibition in multiple Articles. For instance, if a data controller obtains consent without informing the data subject that they can withdraw their consent, we might say that the controller is infringing Article 4(11), which defines consent as "informed'', Article 6(1)(a) which requires consent as a lawful basis, Article 7(3) which imposes the duty to inform about revocability of consent, and Article 13(2)(c) on the transparency duty to inform data subjects – among other things – about the revocability of consent. Infringing at least four provisions seems a very severe infringement, however, all these Articles refer to the same identical rationale (informing about consent revocability and enabling the exercise of this right). Does it mean that this duty is much more important than others? Interpreters might disagree on this answer. On a similar point, the CJEU affirmed that if one data processing activity infringes multiple provisions of the GDPR, this should not allow claimants to "double-count" the harm they suffered.[91] However, there are clear cases where one conduct infringes multiple provisions and duties in different articles or laws which are based on different rationales and principles. In that case, a single conduct that infringes different rules might refer to a very serious interference with the fundamental rights implemented in those secondary laws.

[86] ''(...) *the longer the duration of the infringement, the more weight the supervisory authority may attribute to this factor*'', European Data Protection Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.1 Adopted on 24 May 2023, https://www.edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf, p. 19.

[87] Case Storck v. Germany, No. 61603/00 (Eur. Ct. H.R. June 16, 2005).

[88] Yeung and Bygrave, 146, explicitly refer to "scale" as a possible severity parameter, although they are critical against measurability parameters.

[89] We refer here to the potential number of people involved by a violation, not the number of people potentially or actually *affected* (i.e. people who might report a consequence in their life, a damage or an adverse effect as a consequence of that violation). The number of people affected is part of another parameter. See below Section 3.3

[90] Article 83(3) GDPR states: "*If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*''.

[91] CJEU Case C-741/21, 11 April 2024, ECLI:EU:C:2024:288

3.3. Subjective perception of the severity of an infringement

This section introduces the second parameter - the subjective perception of the severity of an infringement. It evaluates how the infringement of the rules indicated by legislators and courts is reflected in the "social meaning" of a right,[92] i.e. how it is perceived by the dynamic sensitivity of the society, by the specific "group" of impacted people, and by the single impacted individual.

As already affirmed in Section 2, "objective" parameters are not sufficient to determine the severity of some interferences with fundamental rights for several reasons. First, the laws implementing fundamental rights do not always indicate how to assess the severity of some infringements, i.e. they do not set a hierarchy of infringement severity. Second, the interpretation of legal provisions is never unequivocal and many possible nuances depend on the sensitivity of the interpreters themselves. Third, since fundamental rights are aimed at protecting human dignity, their interpretation is inherently dynamic,[93] and depends on the evolving sensitivity in society.[94] Moreover, scarce knowledge, risk perception and attitudes (e.g., risk-prone or risk-averse approach) or potential confirmation bias further confirm the inherent subjectivity of impact assessments.[95]

Accordingly, in this subsection, we suggest considering as a parameter how the infringement of the rules indicated by legislators and courts is perceived, taking into account the dynamic sensitivity of the society, but also by the specific "group" of impacted people and, ultimately, by the single impacted individual. Subjectivity can be perceived and analysed from these three different perception levels: societal, group and individual levels. These three levels are often mentioned in risk management methodologies.[96]

Table 2. mentions the parameters relevant for this subjective assessment of the severity of infringement, in particular, societal perception, group identity perception and individual perception.

Table 2
Subjective parameters and sub-parameters to assess the severity of a legal infringement.

Subjective parameters to assess the severity of infringement of law	Sub-parameters
Societal Perception	professional expert resources; data and expert analysis from academic and empirical studies and civil society groups; statistics; societal/ political thresholds
Group Identity Perception	right-holders; their representatives, especially from groups mostly affected due to, e.g., their historical marginalisation other relevant parties and experts
Individual Perception	impacted individuals; concrete representatives of impacted individuals

3.3.1. Societal perception

When employing this parameter, we can allude to a normative assessment of social significance, as articulated by the Advocate General Sánchez-Bordona in its Opinion on the Austrian Post Case C-300/2 regarding "*the perception prevailing in society at a given time*''.[97] This social perception parameter offers more flexibility, in particular when there is no legislation syndicating a concrete violation of a fundamental right.

To capture the societal perception of the severity of a legal infringement, it is recommended to consult credible, independent professional expert resources,[98] and knowledge coming from data and expert analysis.[99] This knowledge and resources can originate from various sources, ranging from academic scholars and diverse experts or representatives from civil society that have the means to provide the "best available information and scientific insights'' and can "test their assumptions with the groups most impacted by the risks and the measures they take".[100] Moreover, resources can encompass representative statistics, societal thresholds, political evaluations, and user-perceived

[92] The concept of "social meaning" of fundamental rights violations has a long tradition in the field of antidiscrimination. See, one of the first mentioning of the concept in Aaron Antonovsky, "The Social Meaning of Discrimination." Phylon (1960-) 21, no. 1 (1960): 81–95. https://doi.org/10.2307/273741. The theory was then expanded by Deborah Hellman, *Equal Protection in the Key of Respect*, 123 Yale Law Journal, 3036–3062 (2014),3045, who (when commenting Bruce Ackermann, *We the People, Volume 3: The Civil Rights Revolution*. Harvard University Press, 2014, 132) affirms that the "social meaning" is the "general knowledge of our culture and its interpretive practices", also called "situation sense". See also, Deborah Hellman, Discrimination and Social Meaning in The Routledge Handbook of the Ethics of Discrimination, edited by Kasper Lippert-Rasmussen (2018), Available at SSRN: https://ssrn.com/abstract=3047432.

[93] See, Karen Yeung and Lee Bygrave, 143.

[94] ECHR Practical Guide on Admissibility Criteria, Updated on 31 August 2023, p. 83 https://www.echr.coe.int/documents/d/echr/admissibility_guide_eng

[95] Kloza et al., *What could possibly go wrong? On risks to the rights and freedoms of natural persons in EU data protection law, their typologies and their identification*, Technology and Regulation, 2024, p. 318.

[96] As put by CPL in its ''Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU'', the framework for identifying covered high-risk AI applications should involve the use of impact assessments designed to assess the likelihood, severity and scale of the impact of the AI use. Such impact assessments would include the following considerations: severity and likelihood of harm to individuals, groups, or society at large (relying on conclusions that can be reached with reasonable certainty), p. 2, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_risk-based_approach_to_regulating_ai_22_march_2021_.pdf

[97] UI v Österreichische Post, Case C-300/21, ECLI:EU:C:2022:756, para 116.

[98] Guiding Principle 18 of the UN Guiding Principles on Business and Human Rights states that to assess actual or potential adverse impact to human rights, it is needed to consult credible, independent expert resources, including human rights defenders and others from civil society. It reads as follows: ''In order to gauge human rights risks, business enterprises should identify and assess any actual or potential adverse human rights impacts with which they may be involved either through their own activities or as a result of their business relationships. This process should: (a) Draw on internal and/or independent external human rights expertise; (b) Involve meaningful consultation with potentially affected groups and other relevant stakeholders, as appropriate to the size of the business enterprise and the nature and context of the operation. Commentary: The purpose is to understand the specific impacts on specific people, given a specific context of operations. (...) In this process, business enterprises should pay special attention to any particular human rights impacts on individuals from groups or populations that may be at heightened risk of vulnerability or marginalization, and bear in mind the different risks that may be faced by women and men. (...) To enable business enterprises to assess their human rights impacts accurately, they should seek to understand the concerns of potentially affected stakeholders by consulting them directly in a manner that takes into account language and other potential barriers to effective engagement. In situations where such consultation is not possible, business enterprises should consider reasonable alternatives such as consulting credible, independent expert resources, including human rights defenders and others from civil society. The assessment of human rights impacts informs subsequent steps in the human rights due diligence process.'' UN Human Rights Council "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

[99] DIHR, Phase 3: Analysing Impacts section of the Guidance on Human Rights Impact Assessment of Digital Activities, p. 6.

[100] Recital 90 DSA.

risks from scientific empirical studies,[101] among other elements that confer a founded lack of compliance with the law across groups or communities. The weight of professional sources can enhance the subjective social perceptions of an infringement, leading to a quasi-objective societal perception.

Limitations of the parameter

While using subjective social perception to assess the severity of a legal infringement offers flexibility and incorporates societal norms, limitations exist. Bias in media reporting, for example, prejudice and misinformation, may distort perceptions of severity. It can be challenging to capture the heterogeneity of social perceptions comprehensively at various levels (political, cultural, etc.), especially in multicultural societies, even with access to the studies mentioned above. In addition, we affirmed that to understand a societal perspective on infringement severity, we could refer to the result of expert evaluation.[102] Although the reliance on experts' opinions is necessary, such reliance is often theoretically and morally problematic because it is a way to dissimulate purely political considerations under the technocratic shield of "scientific expertise".[103] In addition, we are cognizant that relying on experts might be just a "Chinese box exercise", where we shift the difficulty of delegating a parameter to an external entity ("the experts") that might magically solve this conundrum for the power of their authority.

3.3.2. Group identity perception

Any model aiming to measure the severity of fundamental rights stemming from a legal violation must consider how not only society at large but also how its constitutive impacted communities subjectively perceive such an infringement, especially communities who experience marginalisation and oppression.[104] Therefore, evaluating group identity or stakeholder perception should be considered as an assessment parameter. Moreover, groups have entitlements to have their rights respected, including those pertaining to addressing adverse impacts resulting from legal violations.[105]

Pursuant to assessing the perceived severity of an infringement by a group, we propose the conceptual construct of *group or collective identity* (CI). Group or collective identity is an individual's cognitive, moral, and emotional connection with a broader community, category, practice, or institution.[106] Collective identity is a widely studied concept across academic disciplines,[107] and it is adapted to the legal context as well. There are many types of, and contexts for, collective identity, including religious identity, philosophical identity, gender identity, (sports) fan identity, labour movements, social movements such as African-American civil rights, women's suffrage, LGBT+ rights, political identities, racial and ethnic identities, national and cultural identities, and ideologies.[108] There is a growing field of technical methodologies to analyse the psychological aspect of groups' identity and groups' perceptions.[109]

Stakeholder engagement is critical in fundamental rights impact assessment and includes groups such as rights-holders, duty-bearers, and other relevant parties.[110] The Danish Institute of Human Rights (DIHR) overview regarding the various stakeholders involved in impact assessments holds significance within our group perception model.

i) Right-holders

[101] Jakobi et al. consider that user-perceived privacy risk (a risk referring to a fundamental right violation) can be drawn from an empirical study approach that is able to provide evidence-based policy making (with the use of focus groups and international experts from various disciplines, countries, institutions, and positions); Timo Jakobi, Maximilian von Grafenstein, Patrick Smieskol, Gunnar Stevens, A Taxonomy of user-perceived privacy risks to foster accountability of data-based services, Journal of Responsible Technology, Volume 10, 2022, 100029, ISSN 2666-6596, https://doi.org/10.1016/j.jrt.2022.100029.

[102] See Mantelero, *Beyond Data, Human Rights, Ethical and Social Impact Assessment in AI*, Springer, 2022, 54.

[103] About the risks of relying on "science", see the provocative reflections in the Science and Technology Studies, e.g. Bruno Latour, *The Pasteurization of France followed by Irreductions*. Cambridge, MA: Harvard University Press, 1984 affirming that "science is politics by other means". See also Eve Seguin, Laurent-Olivier Lord; "Bruno Latour's *Science Is Politics By Other Means*: Between Politics and Ontology", *Perspectives on Science* 2023; 31 (1): 9–39.

[104] See, in particular, Ngozi Okidegbe, To Democratize Algorithms, 69 UCLA L. REV. 1688 (2023); Hannah Bloch-Wehba, Algorithmic Governance from the Bottom Up, 48 BYU L. REV. 69 (2022). Meg Young, Lassana Magassa, & Batya Friedman, Toward inclusive tech policy design: a method for underrepresented voices to strengthen tech policy documents, Ethics & Info. Tech. (2019). See also SASHA COSTANZA-CHOCK, DESIGN JUSTICE: Community-Led Practices to Build the Worlds we Need (2020).

[105] See, e.g., Margot E. Kaminski, and Gianclaudio Malgieri, "Impacted Stakeholder Participation in AI and Data Governance", Forthcoming on Yale Journal of Law and Technology (2024-2025), Available at SSRN: https://ssrn.com/abstract=4836460.

[106] Polletta F, Jasper JM (2001) Collective identity and social movements. Ann Rev Sociol 27:283–305.

[107] Extensive experimental research in social science, political science, psychology, biology, geography, anthropology, religion, criminology, philosophy, and economics shows that CI influences human decision making. Cedeno-Mieles, V., Hu, Z., Ren, Y. et al. Networked experiments and modeling for producing collective identity in a group of human subjects using an iterative abduction framework. Soc. Netw. Anal. Min. 10, 11 (2020). https://doi.org/10.1007/s13278-019-0620-8 , p. 2.

[108] Idem.

[109] See, e.g. Velichko H. Valchev, Fons J.R. van de Vijver, Deon Meiring, J. Alewyn Nel, Carin Hill, Sumaya Laher, Byron G. Adams,Beyond Agreeableness: Social–relational personality concepts from an indigenous and cross-cultural perspective, Journal of Research in Personality, Volume 48, 2014,17-32,https://doi.org/10.1016/j.jrp.2013.10.003. See also Adams, B. G., Abubakar, A., Van de Vijver, F. J. R., De Bruin, G. P., Arasa, J., Fomba, E., Gillath, O., Hapunda, G., Looh La, J., Mazrui, L., and Murugami, M. (2016) Ethnic Identity in Emerging Adults in Sub-Saharan Africa and the USA, and Its Associations with Psychological Well-Being. J. Community Appl. Soc. Psychol., 26: 236–252. doi: 10.1002/casp.2247.

[110] The Danish Institute of Human Rights, Analysing Impacts section of the Guidance on Human Rights Impact Assessment of Digital Activities, https://www.humanrights.dk/sites/humanrights.dk/files/media/document/HRIA%20Toolbox_Stakeholder%20Engagement_ENG_2020.pdf p. 6. See also Nicholas Martin, Ina Schiering, Michael Friedewald, Methoden der Datenschutz-Folgenabschätzung: Welche Unterschiede weisen die verschiedenen methodischen Ansätze auf?, 2020, Datenschutz und Datensicherheit - DuD. 44. 154-160. 10.1007/s11623-020-1242-z.

Right-holders[111] can be workers, supply chain workers, local community members including women, children, indigenous peoples, LGBT+ persons, migrants, persons with disabilities, human rights defenders, consumers, and end-users. This category can also include organisations or entities, such as trade unions or religious institutions that may act in a representative capacity of groups potentially impacted. For instance, it is important to recognize a consumer group's reasonable expectations regarding the quality, performance, or terms of delivery of a consumer service,[112] and consumer awareness regarding the negative outcomes that may arise following the purchase or use of a good or service[113] through consumer complaints, consumer perception research or consumer survey results *vis a vis* industry norms.

ii) Other relevant parties and experts

Other parties may include individuals or organisations whose group knowledge or views could assist in the assessment of fundamental rights impacts resulting from a legal infringement. They may include specialist representatives from multilateral organisations (e.g., the UN or the International Labour Organization); national human rights institutions; NGOs and civil society organisations (CSOs); local, regional, and international human rights mechanisms and experts;[114] and rights-holder representatives or representative organisations. They might also include other duty-bearers, i.e. private or public entities with similar human rights duties or responsibilities towards rights-holders as required by specific laws implementing fundamental rights.

Limitations of the parameter

Collective identities may be transient over short time scales and may ebb and flow over longer time scales.[115] Consequently, a person's identity may include a combination of dynamically changing, hierarchical collective identities, which requires updated studies of the collective identity in a given field, hampering its inclusion in a group. In addition, group perceptions might be biased depending on the specific variables of a historical, social, or political context and might lack foreseeability (or even reasonableness). However, we believe that social scientists experts in analysing group perceptions might play a reasonableness test to avoid potential distortive effects.

3.3.3. *Individual perceptions*

There is a more granular element of perception to be considered: the perception of the severity of infringement at the individual level of the single impacted person. This parameter is different from the group identity perception, because it is not based on specifically identified (e.g., historically marginalised or chronically impacted) groups, but on potential concrete samples of impacted individuals. In other words, individual perception should not be collected on the basis of groups who experience a common identity (on a psychological, social or historical basis), but on concrete representatives of individuals who might be impacted in the specific case, regardless of their group identity or of their belonging to specific minorities.

In *ex post* analyses about the impact of fundamental rights in specific cases, e.g., in a court, it is possible to consider the perception of the individual (e.g., the plaintiff). Indicators based on the perceptions, opinions, assessment, and judgement of the right-holders, and those of their legitimate representatives or proxies who were scoped by an infringement, are categorised as subjective indicators and are to be accounted for in the assessment of impact severity.[116] The subjective judgement could be, for example, an assessment expressed in a narrative form of how independent and fair the judiciary is.[117] Examples of subjective perceptions that can assist in the severity assessment of legal infringement could consist of feelings (less severe than directly quantifiable psychological damages) of being offended, annoyance, anger, and loss of confidence.[118] Other proxies for subjective perception of the severity of an infringement might consist of indignation,[119] fear,[120] uncertainty,[121] or feelings of injustice.[122]

In *ex ante* impact assessments, this analysis might be more challenging, considering the difficulty of singling out specific individuals that might be concretely impacted (in the future) by potential practices, services or products. Nevertheless, data controllers are obliged to

[111] The Danish Institute for Human Rights elaborates that regarding the views and perspectives of the rightholders, the perceptions of the affected individuals may or may not correlate with what constitutes a human rights abuse under international human rights law. Thus, individual and group perceptions of impact should be taken into account but should not be considered determinative. Individuals and/or groups may perceive that they are negatively impacted in a certain way, even when that impact does not amount to a negative human rights impact. Conversely, individuals and/or groups may perceive that they are not negatively impacted when other data and expert analysis suggest that their rights have been impacted, or the impacted individuals may simply not know that their rights have been or could be impacted even when they have. In other words, it can be an issue of knowledge rather than perception. For example, individuals or groups might claim that their content posted on social media is being 'demoted', and that their freedom of expression has therefore been negatively impacted. However, the evidence suggests this has not happened and it simply was not a post that garnered a lot of interactions and therefore did not spread or 'go viral'. Yet another example, where an individual's right to privacy can be negatively impacted if data is collected by a digital platform the individual is using. The individual feels safe because the platform clearly states that it anonymises all data it collects. However, if the data anonymisation is flawed, the data can be reidentified and sensitive data related to the individual might be accessed by third parties. In this case the individual is likely to not know that the impact is occurring, in Phase 3: Analysing Impacts section of the Guidance on Human Rights Impact Assessment of Digital Activities p. 6.

[112] The ''reasonable expectations of consumers'' is a parameter to measure consumer detriment. Anything that falls short of what consumers reasonably expect, given the circumstances of the transaction, counts as detriment, OECD (2019), Measuring Consumer Detriment and the Impact of Consumer Policy Feasibility study, DSTI/CP(2019)13/FINAL, p.10.

[113] Idem.

[114] Regarding the reliance on human rights experts for human rights impact assessment quantification see Alessandro Mantelero, *Beyond Data*, 54.

[115] Benjamin DJ, Choi JJ, Fisher G (2016) Religious identity and economic behavior. The Review of Economics and Statistics, 98(4):617–637.

[116] The views and perspectives of those who are experiencing them or who may experience them is also to be accounted for in the assessment of impact. UN Human Rights Council "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework" https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

[117] Human Rights Indicators: A Guide for Measurement and Implementation, 2012, https://www.ohchr.org/sites/default/files/Documents/Publications/Human_rights_indicators_en.pdf p.18.

[118] (...) ''Felt offended by the fact that an affinity with the party in question had been attributed to him … [and the] fact that data relating to his supposed political opinions were retained within that company caused him great upset, a loss of confidence and a feeling of exposure. … [N]o harm other than those adverse emotional effects of a temporary nature has been established" Case C-300/21, Österreichische Post, para 12.

[119] A feeling of indignation was felt due to the fact that the claimant's picture was used in the defendant's airport webpage and without informing the claimant, North Holland District Court, Case 8117599 CV EXPL 19-16066, ECLI:NL:RBNHO:2020:8537.

[120] Upon a data breach, the data subject alleged fear fear that her personal data, having been published without her consent, might be misused in the future, or that she herself might be blackmailed, assaulted or even kidnapped a consequence, para 13, Case C-340/21, ECLI:EU:C:2023:986.

[121] Feelings of fear and uncertainty triggered by the fact that their personal data were transferred to Google Inc. in the US, para 35, LG München I - 4 O 13063/22, https://www.gesetze-bayern.de/Content/Document/Y-300-Z-GRURRS-B-2023-N-6354?hl=true

[122] Case Keegan v Ireland (1994), ECHR, Judgement No(s). 16969/90), para 68.

identify potential individuals who are the target of data processing activities, and that need to be involved in an impact assessment consultation process, so that their views or the ones of their representatives are accounted for, pursuant to Article 39(5). It is possible to evaluate specific groups of individuals that might be concretely affected in the future, before the first round of deployment of certain practices, services or products. Herein we provide several examples. Regulatory bodies enforcing their respective legislations already perform monitoring or inspections ex officio[123] on online services to gauge evidence of practices that can have significant impact on users. Regulators and policymakers can independently conduct and/or outsource external studies on potential problematic practices to collect evidence of the effect and impact of specific practices to users in a given context and to a sample of users.[124] Regulators can utilise internal studies or evaluations conducted by online services[125] (for example, through a request for information, as per Article 67 DSA). Such evidence can contain the methodology and results of such evaluations, including, A/B testing that companies perform to assess the potential impact on users and to enhance their services and products. Foresight studies and anticipation techniques are being applied to novel technologies by regulatory bodies to anticipate potential impacts to targeted users exposed to certain technologies.[126]

Limitations of the parameter

It is important to notice that this parameter cannot be properly considered in *ex ante* impact assessments unless the assessor takes a proxy-based analysis of some potentially affected data subjects. In addition, we are aware that the boundary between certain perceptions and some immaterial impact to mental well-being and mental health is not so sharp (e.g., sometimes indignation resulting from suffered infringement can raise depression or psychological disorders). However, this subjective parameter and the parameter of adverse effects on one's mental well-being (see section 3.4 below) have a fundamentally different nature that we can observe in two elements. The first element is the *rationale* of the parameter. Herein, we are just referring to how individuals (as part of society and of their impacted groups) perceive the severity of a legal infringement. They are privileged observers of the seriousness of certain legal misconduct of a (private or public) counterparty, regardless of whether this perception can even give rise to quantifiable psychological adverse effects on them. Human perception and human involvement can portray contextual cues that can be meaningful in the assessment of severity. The second element is the *measurability*. Individual perceptions are closer to "opinions" rather than psychological statuses. While perceptions-opinions can be collected by social science experts or even legal experts, psychological statuses can be diagnosed by medical doctors (psychologists, psychiatrists, etc.).

Table 3
Adverse effects parameters and sub-parameters to assess the severity of a legal infringement.

Parameters to assess adverse effects	Sub-parameters	Instances
Economic	Financial loss	loss of income; financial burden; reduction in the value of property
	Costs of remedies and effort	-
	Loss of economic opportunities	benefits, profit or gains that could have been yielded
Time	Time loss	-
	Duration of effects on affected persons	-
	Time wasted in remedying the violation	-
Scale	Number of people affected	-
	Indirect and potential reach	-
Reversibility	Degree of reversibility	-
Well-being	Physical health	health implications or injuries
	Mental integrity	emotional suffering, loss of amenity
	Loss of life opportunity	right, service, contract, career advancement, educational prospects
	Social well-being effects	effects on social relationships, social status, standing in a community

3.4. Adverse effects (changes in one's life) parameters

After the normative objective and subjective analysis of infringements (analysed in section 3.2 and 3.3 respectively), herein we analyse the possible consequences of those infringements on the daily life of impacted individuals, such as damages, but also other adverse effects on their lifestyle, etc. In this section, we suggest specific, practically defined parameters that can tangibly capture the change in an individual's life due to a legal infringement. We aim to steer clear of ambiguous, non-informative terms, circular definitions, and abstract concepts (e.g., magnitude, intensity, seriousness, etc.) to ensure clarity and precision in this assessment. Severity can be determined by the *consequences* for the individuals concretely affected.[127] In this line, Manterelo[128] defined the concept of "severity of the expected consequences'' considering the nature of potential prejudice in the exercise of rights and freedoms and their consequences. Such changes can either temporarily or permanently diminish the quality of life. In Table 3 we portray our proposed parameters that capture changes in life circumstances, such as economic loss, time, scale, reversibility and well-being.

[123] On 16 January 2019, the Belgian Data Protection Authority (DPA) initiated ex officio, without any previous data subject complaint, an investigation into the GDPR-compliance of tracing technologies on some of the most popular Belgian news websites, including knack.be and levif.be, run by the Roularta Media Group. https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-85-2022.pdf.

[124] European Commission, Directorate-General for Justice and Consumers, Francisco Lupiáñez-Villanueva, Alba Boluda, Francesco Bogliacino, Giovanni Liva, Lucie Lechardoy, and Teresa Rodríguez de las Heras Ballell, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2838/859030.

[125] The French Data Protection Authority highlights the significance of using internal evidence of online services, as reflected in the following excerpt: ''processing managers are recommended to organise user tests (with representative panels, for example, or other forms of test that are recognised or even normalised, such as legibility or accessibility) with a view to raising any uncertainties on users' actual understanding. This process of improvement, measurement, evaluation and testing can in fact aim to be an integral part of the accountability strategy of processing managers: the competent authorities could be informed of the results of these tests and assess the relevance with respect to the principles of simplicity and accessibility of information'', CNIL, Shaping Choices in the Digital World. IP Reports Innovation and Foresight N°06, Consulted on 25 July2024, https://www.cnil.fr/sites/cnil/files/2023-06/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf, p. 40.

[126] TechSonar aims to anticipate emerging technology trends from a data protection perspective in Large Language Models (LLM), Extended reality (XR), deepfake detection, internet of behaviors and digital identity wallets, https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar_en

[127] DIHR, Phase 3: Analysing Impacts section of the Guidance on Human Rights Impact Assessment of Digital Activities, p. 5.

[128] According to Mantelero, assessing the consequences of impacts requires considering i) the gravity of the prejudice (gravity), and ii) the effort to overcome it and to reverse adverse effects (effort). Alessandro Manterelo (2022). *Human Rights Impact Assessment and AI. In: Beyond Data*. Information Technology and Law Series, vol 36. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-531-7_2, p. 56.

3.4.1. Economic loss

An adverse effect parameter can refer to economic losses of the affected person due to a legal violation. Economic loss can manifest in different forms:

1. loss of income, financial burdens incurred, and a reduction in the value of property with respect to an individual's assets;[129]
2. money used and effort[130] in remedying the problem for a concrete affected person[131] resulting from a legal infringement, according to their means and resources at a given time;
3. loss of economic opportunities, which can mean benefits, profit or gains that could have been yielded with a certain probability, but became directly or indirectly impossible due to the infringement.

Limitations of the parameter

Individuals affected by a legal violation may have different financial backgrounds and resources, and the impact can vary depending on income level, assets, and access to financial support systems.

3.4.2. Time

Time is a key component in the mensuration of adverse effects as consequences of interferences with fundamental rights. Examples to be contemplated regarding time consist of:

1. time loss as a direct result of the problem,[132]
2. time used in remedying the problem for the affected person; and relatedly,
3. duration of effects on the affected person,[133] and the long-term impact on a person. For example, the fundamental right of human dignity can be measured through the (loss) of quality of time.[134] Consider the case of a senior person repeatedly attempting to resolve a billing issue with their internet service provider through an automated customer service system that only makes use of AI-driven voice response and chatbots. Besides the obvious loss of time, this issue can trigger dependence on others (family and relatives), interruptions of the service, frustration, and confusion.

Furthermore, the duration of an infringement can trigger cumulative impacts affecting the rights of the same individual.[135] Consider cumulative small, same-time, infringements over time (for example, the unlawful use of facial recognition technology in combination with other tools, such as sentiment analysis, speech recognition and analysis, and so forth), and cumulation of infringements related to different rights within the same span of time.

Limitations of the parameter

Regarding point (3), individuals can have inconsistent time preferences regarding their quality of time, which can also be influenced by experience and context, rendering this parameter more volatile. For instance, when someone clicks on their preferred social media site, they may only intend to spend five minutes catching up but can easily get sucked into staying on the site for an hour.

3.4.3. Scale

Scale refers to the target of the infringement, i.e., the person or groups that got negatively affected and, thus, suffered adverse consequences due to an infringement.[136] In fact, violations that affect a large number of people will raise greater supervisory concern than violations that impact a limited number of persons. This parameter also enables the assessment of whether a violation was directed towards or impacted vulnerable consumers and community members, and foresees any actual or potential discrimination to be included in assessing the impact's severity.[137] Such severity assessment requires contemplating differences of impacts to different groups or individuals at heightened risk of becoming vulnerable or marginalised, including women, children, ethnic minorities, persons with disabilities, LGBT+ individuals, and other characteristics. Herewith we consider the number of persons affected by the infringement, as well as the indirect and potential reach.

i) Number of persons affected by the infringement

This parameter is consensual among laws and public reports[138] and refers to the number of persons affected by an infringement,[139] including if such persons belong to marginalised communities.[140] The higher the number of individuals involved, the more weight a decisionmaker may attribute to this factor.[141]

ii) Indirect and potential reach

[129] von Bar, Christian, Clive, Eric and Schulte-Nölke, Hans. *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR). Outline Edition*, Berlin, New York: Otto Schmidt/De Gruyter european law pub, 2009. https://doi.org/10.1515/9783866537279, p. 402.

[130] According to Mantelero, assessing the consequences of impacts requires considering i) the gravity of the prejudice (gravity), and ii) the effort to overcome it and to reverse adverse effects (effort). Alessandro Manterelo (2022). Human Rights Impact Assessment and AI. In: Beyond Data. Information Technology and Law Series, vol 36. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-531-7_2, p.56.

[131] OECD (2019), Measuring consumer detriment and the impact of consumer policy Feasibility study, DSTI/CP(2019)13/FINAL.

[132] Franck Michel, Fabien Gandon. Pay Attention: a Call to Regulate the Attention Market and Prevent Algorithmic Emotional Governance. 2024. ffhal-04479314.

[133] The AIA in Article Art. 3(1)(1)b) refers to the duration of effects when defining significant risk: ''*'significant risk' means a risk that is significant as a result of the combination of its severity, intensity, probability of occurrence, and duration of its effects, and its the ability to affect an individual, a plurality of persons or to affect a particular group of persons.*''

[134] Catherine Dupré, *The Age of Dignity: human rights and constitutionalism in Europe*, 2018, Hart Publishing, 2018 ISBN 10: 1509920013.

[135] See DHIR, Phase 3: Analysing Impacts section of the Guidance on Human Rights Impact Assessment of Digital Activities p. 22.

[136] EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR Version 2.1 Adopted on 24 May 2023.

[137] DIHR report gives the following example: ''an analysis that focuses purely on the number of people affected might identify that for three identified actual impacts of a digital product, five out of 100 people experience each impact; however, if the five people impacted are always e.g. women human rights defenders, this should be observed in the analysis, as it may be due to systemic persecution against the particular group of people in the given context'', p. 29; Access Now ''Towards Meaningful Fundamental Rights Impact Assessment under the DSA'', September 2023, accessible at https://www.accessnow.org/wp-content/uploads/2023/09/DSA-FRIA-joint-policy-paper-September-2023.pdf, p. 14

[138] Recital 79 of the DSA states: ''*In determining the significance of potential negative effects and impacts, providers should consider the severity of the potential impact and the probability of all such systemic risks. For example, they could assess (…)* whether the potential negative impact can affect a large number of persons''. This parameter is also supported by several policymakers, such as the OECD, DIHR, and EDPB.

[139] No differentiation should be made between users and non-users of a given service or platform, Access Now ''Towards Meaningful Fundamental Rights Impact Assessment under the DSA'', September 2023, accessible at https://www.accessnow.org/wp-content/uploads/2023/09/DSA-FRIA-joint-policy-paper-September-2023.pdf, p. p. 14.

[140] Access Now ''Towards Meaningful Fundamental Rights Impact Assessment under the DSA'', September 2023, accessible at https://www.accessnow.org/wp-content/uploads/2023/09/DSA-FRIA-joint-policy-paper-September-2023.pdf, p. p. 14.

[141] European Data Protection Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.1 Adopted on 24 May 2023, https://www.edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf, p. 19.

Relatedly, it may be considered that an infringement takes on systemic connotations and can, therefore (potentially), even at different times, materialise in life changes of those who were not directly related by an infringement (like not users of the rogue platform). For example, the dissemination of illegal online content on a platform that perpetuates gender-based online violence or constitutes illegal forms of hate speech can severely harm the right to life, liberty, and security of groups of people who may not be registered users of the platform where the content was distributed. Thus, this parameter can be dynamically used to contemplate potentially affected people.

Limitations of the parameter

This parameter is subject to the necessary context-specific determination of the impacted parties. The overall context in which the infringement occurred needs to be considered since local circumstances may differ by region and by the specificity of groups of people. It also seems difficult to define a scale with fixed ranges of rightsholders in relation to affected groups. For example, differences in life situations (in earnings and job histories) among men and women might often be linked to different insurance risks and credit loans that can be used in gender discrimination in insurance pricing.[142]

3.4.4. Reversibility or reparability

Reversibility and the related remediability of impacts is a recurrent parameter in both legislation[143] and policy reports.[144] It refers to the ability, whether positive or negative, to repair and/or restore impacted individuals to a situation at least the same as, or equivalent to, their situation before the impact.[145]

Furthermore, if an action is capable of being remedied, another criterion to consider is the extent to which it can be reversed, or the *degree of reversibility*, i.e., how difficult it is to restore and/or remedy the situation prevailing before the potential impact.[146] The degree of reversibility is confirmed by Mantelero, who explains that the variable "effort" entails the effort to overcome the prejudice and to reverse adverse effects.[147]

Consider the example of the unlawful demolition of a person's home without adequate notice, fair compensation, or alternative housing, leaving that person and their family homeless and without their possessions destroyed during the demolition. The degree of reversibility varies if a home and compensation are to be provided. Another example involves a company utilising an AI-powered recruitment system to screen job applicants. The system, trained on biased data that reflects historical discrimination patterns, disproportionately rejects qualified candidates based on their last name, race, and gender. While such a company can rectify its hiring practices when it is aware of or upon complaints/audit, the loss of employment for the affected applicant(s) might be fully recovered.

Limitations of the parameter

Reversibility is hard to operationalise ex ante. It would require assessing the pre-impact status in terms of feasibility, time frame demanded for restoration, effort needed to reverse, long-term consequences in many and diverse scenarios wherein the access to past case studies or availability of historical data may be inexistent. However, as most exante analysis, it would require efforts in predicting potential effects as concretely as possible and anticipate whether these effects are reversible or not. Furthermore, remediability or reversibility of impacts must be timely and effectively identified to prioritise, prevent and mitigate the most severe impacts to intangibles or those where a delayed response would hinder remediation. Restoration may not always be possible when the impact has a permanent consequence for people. Remediation may be judicial, and expert advice should be sought in the specific context.

3.4.5. Well-being

An infringement might reflect a change in a person's well-being, and the following parameters can assist in assessing the severity of such interference: physical health, mental integrity, loss of life opportunity, and social well-being effects. Below we discuss the parameters and their potential limitations.

Physical health. An infringement may raise physical health implications or injuries. The impact of such injuries is contingent upon subjective factors, including individual pain thresholds and underlying health conditions. Some physical health impacts might not be immediately apparent and could manifest long after the infringement, and it would require evaluation and reporting of such physical changes in time.

Mental integrity. Mental integrity can consist of pain and suffering, and impairment of the quality of life.[148] Emotional suffering or loss of amenity reflect changes in one's life.[149] In many instances, the ECtHR has found that an applicant has suffered moral damage as a result of an infringement of the Convention. Interestingly, the CJEU has recently affirmed that (at least for what concerns the fundamental right to data protection) physical injuries are not by their nature more serious than moral or psychological damages.[150] It has held that the impact of the violation may be regarded as being of a nature and degree as to have 'impinged so significantly the moral well-being of the applicant as to require something further' and that 'moral damage occurred as a result of the infringement of fundamental human rights'.[151]

[142] European Commission (2012), EU rules on gender-neutral pricing in insurance industry enter into force, Press release, IP/11/1581, 20 December 2012.

[143] Recital 79 of the DSA reads ''In determining the significance of potential negative effects and impacts, providers should consider the severity of the potential impact and the probability of all such systemic risks. For example, they could assess (...) its potential irreversibility''. Article 83(2)(c) of the GDPR refers to ''any action taken by the controller or processor to mitigate the damage suffered by data subjects.

[144] DHIR, Phase 3: ''Analysing Impacts section of the Guidance on Human Rights Impact Assessment of Digital Activities',' p. 26; Guiding Principle 14 scopes the extent of impact severity. The principle refers that ''Severity of impacts will be judged by their scale, scope and irremediable character. The means through which a business enterprise meets its responsibility to respect human rights may also vary depending on whether, and the extent to which, it conducts business through a corporate group or individually (...).''; and Access Now ''Towards Meaningful Fundamental Rights Impact Assessment under the DSA'', September 2023, accessible at https://www.accessnow.org/wp-content/uploads/2023/09/DSA-FRIA-joint-policy-paper-September-2023.pdf, p. 14-15.

[145] It is often the case that the greater the scale of an impact, the less it is 'remediable'.

[146] Recital 79 of the DSA states that ''[I]n determining the significance of potential negative effects and impacts, providers should consider the severity of the potential impact and the probability of all such systemic risks. For example, they could assess (...) how difficult it is to remedy and restore the situation prevailing prior to the potential impact.'

[147] Alessandro Manterelo (2022). *Human Rights Impact Assessment and AI. In: Beyond Data*. Information Technology and Law Series, vol 36. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-531-7_2, p. 56.

[148] von Bar, Christian, Clive, Eric and Schulte-Nölke, Hans. *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR). Outline Edition*, Berlin, New York: Otto Schmidt/De Gruyter european law pub, 2009. https://doi.org/10.1515/9783866537279, p. 396.

[149] Clemente, Miguel, and Dolores Padilla-Racero. "The effects of the justice system on mental health." Psychiatry, psychology, and law: an interdisciplinary journal of the Australian and New Zealand Association of Psychiatry, Psychology and Law vol. 27,5 865-879. 5 May. 2020, doi:10.1080/13218719.2020.1751327.

[150] See CJEU, C-182/22 and 189/22, *Scalable Capital*, 20 June 2024, paras. 37-39.

[151] In relation to the right to life, and right to liberty and security, see the case Varnava and Others v Turkey , 18.9.2009, Nos. 16064/90, para. 224.

For example, when it comes to targeted advertising, consumers need to be informed that they can opt-out of being targeted. Upon an infringement of this legal requirement, they might be subjected to advertising they do not want nor expect. This is particularly problematic in combination with highly sophisticated AI systems for advertising which can amount to some sort of manipulation of consumer preferences and discrimination.[152] Recently, the CJEU noticed that even the "fear" of a data subject about the risk of "losing control of one's own personal data" can be considered a damage as a consequence of a violation of the fundamental rights to data protection.[153]

Loss of life opportunity. Opportunity losses could consist of exercising a right, using a service or benefiting from a contract, career advancement, or educational prospects. Assessing potential missed opportunities involves reliable methods (e.g. foresight and anticipatory studies, qualitative analysis considering individual experiences through surveys, interviews, and longitudinal studies, although interpretation remains inherently subjective and dependent on one's resilience and individual circumstances).

Social well-being effects. Social well-being effects on social relationships, social status, and standing within the community due to the infringement could be qualified as changes in one's life. Needless to say, social well-being is influenced by cultural norms and values, leading to variability in assessments across different cultural contexts. Objective data and subjective experiences could evaluate such changes.

Limitations of the parameter

The different holistic aspects of well-being can often be found to be intertwined. For instance, a decline in mental health can affect physical health and vice versa, and thus, isolating the impact of an infringement on a single dimension can be difficult. However, resorting only to quantifiable sciences to measure well-being runs the risk of reducing actionable different variables to Chinese box concepts or "zombie nouns".[154]

4. Conclusion

The goal of this article is to provide a parameter-based framework to operationalise the assessment of the impact on fundamental rights, recognizing the crucial need to conduct fundamental rights impact assessments as mandated by the GDPR, DSA, and AI Act. This goal is also essential to apply transversal concepts, such as human vulnerability, from a fundamental rights perspective. This endeavour seeks to bridge the gap between legal mandates and practical implementation, ensuring robust protection for individuals within the digital ecosystem.

In the ongoing intellectual debate between the risk-of-harm-based approach and the risk-of-violation (or right-based) approach to impact assessment, we adopt the latter, as it aligns with the core of fundamental rights. However, our goal is to operationalize this approach effectively. While *violations* are clear-cut, the concept of *interferences* with fundamental rights is more nuanced and measurable, as acknowledged by the European Courts. Violations function as a binary parameter (yes-or-no), whereas interferences are a spectrum (from mere contact to violation). This spectrum *can* be measured to prioritise actions on higher risks, mitigate higher human vulnerabilities, and conduct meaningful impact assessments, as requested by EU law.

Accordingly, we propose a comprehensive framework for analysing interferences, identifying three high parameters, alongside more granular parameters necessary for a thorough assessment. We emphasise the need to avoid ambiguous terms, vague definitions, or self-referential loops when defining the impact on fundamental rights. Recognizing that fundamental rights are not material objects but principles aimed at preserving dignity, we incorporate parameters that capture their legally, politically, socially, and culturally situated nature.

We propose objective parameters considering how legislators interpret, implement, and substantiate specific fundamental rights through secondary legislation, statutes, regulations, and acts. Judicial interpretations of these laws also play a crucial role in shaping the assessment. Secondly, we suggest evaluating how infringements of these rules are perceived by society, impacted groups, and individuals, including the dynamic sensitivity of these perceptions. Lastly, we propose analysing the tangible consequences of these infringements on individuals' daily lives, encompassing traditional damages and other adverse effects on their lifestyles.

Our approach mensures a comprehensive evaluation of interferences with fundamental rights, guiding both deployers of services but also policymakers in protecting these rights within the digital ecosystem. This framework acknowledges the complex, multifaceted nature of dignity and fundamental rights, promoting for a more holistic and effective methodology for assessing and addressing potential risks, as legally required.

Declaration of competing interest

No conflict of interest to declare

Acknowledgments

Partially funded by the Project RESOCIAL, funded by NWO and ZonMW, NWA.1540.21.001. We are grateful for the great feedback received within TILTing Perspective 2024 and at SciencePo in October 2024 and especially by Dr. Silvia De Conca, Maciej Otmianowski, Prof. Niels van Dijck, Prof. Alessandro Mantelero, Itxaso Dominiguez de Olazabal, Dr. Michele Loi, Vanja Skoric, Dr. Raphael Gellert, Dr. Raphaële Xenidis, Dr. Lucas Costa dos Anjos.

Data availability

No data was used for the research described in the article.

[152] Fundamental Rights Agency. Agency, Getting the Future Right: AI and Fundamental Rights (2020), [https://perma.cc/Z], p. 80.

[153] See CJEU, Case C-200/23, Agentsia po vpisvaniyata v OL, 4 October 2024, par. 144,

[154] Steven Pinker, The Sense of Style, 318.