Book Section:
Siapka, A., Tzanou, M. orcid.org/0000-0001-5360-2038 and Nelson, A. (2024) Re-imagining data protection: Femtech and gendered risks in the GDPR. In: Costello, R. and Leiser, M., (eds.) Critical Reflections on the EU's Data Protection Regime: GDPR in the Machine. Hart Studies in Information Law and Regulation . Hart Publishing (Bloomsbury Publishing) ISBN 9781509977840

5

Re-imagining data protection: Femtech and gendered risks in the GDPR

Anastasia Siapka, Maria Tzanou and Anna Nelson

I. Introduction

The European Union's (EU's) General Data Protection Regulation (GDPR)[1] is considered 'the gold standard' for data protection laws worldwide.[2] Yet, it is a truism to state that it neglects gender. The Regulation itself adopts a gender-neutral approach: gender is notably missing from the specific provisions about the types of information revealing special category data as well as from the GDPR in general.[3] Academic debates on the GDPR (or data protection more broadly) and gender are also limited,[4] with the notable exception of Malgieri's and González Fuster's research into whether the 'gendered data subject' could be considered as 'vulnerable'.[5]

This chapter aims to address this regulatory and knowledge gap: it investigates the GDPR from a gender perspective to question whether the Regulation does/should explicitly recognise gender and, if so, how. In this regard, it makes three distinct contributions to the literature: First, it argues that gender *matters* within the GDPR. Using Femtech as a case study at the intersection of data protection and reproductive

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (GDPR) [2016] OJ L119/1.

[2] See, inter alia, G Buttarelli, 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard' (2016) 6 *International Data Privacy Law* 77.

[3] Despite sex being a protected characteristic in EU anti-discrimination law, it is absent from GDPR, art 9 or any other GDPR provision. As explained in III.2, this omission is not merely formal or linguistic but rather reveals a substantive gap in the role that data protection rights (may) hold for the protection of sexual and reproductive rights.

[4] Jens T Theilen et al, 'Feminist Data Protection: An Introduction' (2021) 10 *Internet Policy Review* 1; Maria Tzanou, 'The Future of EU Data Privacy Law: Towards a More Egalitarian Data Privacy' (2020) 7 *Journal of International and Comparative Law* 449; Gloria González Fuster, 'Feedback to the Consultation on the White Paper on AI- Focusing on AI & Gender: An EU Law Perspective' (2020).

[5] Gianclaudio Malgieri and Gloria González Fuster, 'The Vulnerable Data Subject: A Gendered Data Subject?' (2022) 13 *European Journal of Law and Technology* 1, 1.

and sexual rights, we show that technology-facilitated gendered surveillance is inextricably linked with the sexual and reproductive rights of women and girls (or the lack thereof). The GDPR's gender blindness thus reveals a further omission: a lack of acknowledgment of the significance of data protection rights for the safeguarding of women's sexual and reproductive wellbeing and autonomy.[6] The GDPR's gender-blind approach fails to recognise that personal data (and data gaps),[7] as well as data subjects, and risks of processing can be *gendered*.

Second, the chapter argues that *gendered risks* should be encompassed by the GDPR's risk-based approach. In this regard, we first examine *in abstracto* the GDPR's risk-based approach, evaluating its conceptual limitations, interpretative gaps and practical implementation difficulties. We then articulate a conceptualisation of *gendered risks* for the first time in the data protection scholarship and identify types of gendered risks that are not currently captured by the GDPR's narrow focus on *individual* risks: these include *embodied*, *collective* and *societal* gendered risks.

Third, the chapter argues that the GDPR *should* be made gender responsive by explicitly acknowledging *gendered risks*. Such a recognition is significant for *symbolic* and *normative* reasons. We then re-imagine the GDPR and explore how this legislative framework could account for gendered risks *de lege ferenda*. Recognising that this re-imagination of the GDPR would require legislative intervention, we also offer a more moderate re-thinking of this instrument, placing gendered (especially collective) risks at the forefront of data protection. The proposed re-thinking of the GDPR both *de lege ferenda* and *de lege lata* provides several ways that legislators, courts, regulators and also data controllers could incorporate gendered risks in the interpretation, application and implementation of the GDPR.

[6] We recognise that not all those who menstruate, conceive and use 'femtech' are women, and that the impact of gendered risks may also be experienced by people who are not women. Further, we recognise that transgender men and non-binary individuals may face specific risks that are not captured by our analysis.

[7] Caroline Criado Perez, *Invisible Women: Exposing Data Bias in a World Designed for Men* (Vintage 2019).

The chapter is structured as follows: Part II examines the GDPR's risk-based approach, highlighting its conceptual ambiguities, the tension between risks and rights and the over-reliance on data controllers. Part III turns to the gendered risks that this approach has so far overlooked. It employs femtech as a case study of everyday techno-management of women's sexual and reproductive realities to explain why such experiences raise gendered concerns which are very relevant to data protection law. Part IV re-imagines the GDPR so that it becomes gender responsive. It introduces a definition of *gendered risks* and identifies different types thereof using examples from the femtech context. It then discusses the *symbolic* and *normative* significance of an explicit recognition of gendered risks within the GDPR. Finally, Part V concludes and reflects on future research.

II. Risk in the GDPR

(i) The GDPR's risk-based approach

Within the GDPR, risk serves a dual role: as an object of regulation *and* a feature of the regulatory approach.[8] The former renders the GDPR a 'risk regulation', aiming to mitigate the risks of data-driven technologies and proactively safeguard individuals' rights.[9] The latter entails that the GDPR adopts a 'risk-based approach', implying the specific ways in which its provisions should be implemented to achieve these aims.[10]

[8] Risk was not foreign to the GDPR's precursor, the Data Protection Directive (DPD), particularly concerning the security of processing (art 17) and checks by supervisory authorities (art 20). Risk has likewise implicitly justified the categorisation of certain personal data as special categories thereof (art 8): their sensitive nature increases the risk of adverse or discriminatory impacts, necessitating stricter conditions for their processing. However, it now permeates the GDPR throughout, holding a more prominent and functional role, as explained below.

[9] Claudia Quelle, 'The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too' in Ronald Leenes et al (eds) *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2017) 33–62.

[10] ibid.

Risk-based approaches facilitate and justify resource allocation based on the potential impact and likelihood of risks.[11] They allow regulators to 'channel their resources to those issues which pose the greatest risk to the achievement of their objectives', thereby enhancing efficiency.[12] Similarly, by dismissing unnecessarily burdensome obligations, the GDPR's risk-based approach seeks to ensure that data protection is effectively implemented.[13] Risk is integral to the accountability principle (GDPR, art 5(2)), which assigns data controllers the responsibility for ensuring and demonstrating that personal data processing complies with data protection principles.[14] The risk-based approach shapes this responsibility by both forming and triggering controllers' obligations.[15]

First, risk determines the technical and organisational measures controllers must implement for compliance. These measures should consider 'risks of varying likelihood and severity for the rights and freedoms of natural persons'.[16] Controllers need not implement all possible or the most demanding measures in every case (e.g., even for small-scale, simple processing).[17] Rather, their accountability admits different levels, corresponding to 'the facts and circumstances of each particular case'.[18] Accountability obligations are then scalable, meaning that their scope is commensurate with the risk of the processing: higher or lower likelihood and severity of said risk warrant proportionately more or less demanding obligations.[19] Akin to 'calibrating' shooting equipment based on observed hits, controllers 'calibrate' their

[11] Julia Black and Robert Baldwin, 'Really Responsive Risk-Based Regulation' (2010) 32 *Law & Policy* 181 cited in ME Gonçalves, 'The Risk-Based Approach under the New EU Data Protection Regulation: A Critical Perspective' (2020) 23 *Journal of Risk Research* 143.
[12] J Black, 'Risk-Based Regulation: Choices, Practices and Lessons Being Learnt' in OECD, *Risk and Regulatory Policy* (OECD Publishing 2010) 185–236, 186; cited in Gonçalves, ibid at 143.
[13] Article 29 Data Protection Working Party, 'Opinion 3/2010 on the Principle of Accountability' (WP 173, 13 July 2010); Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (WP 218, 30 May 2014).
[14] Article 29 Data Protection Working Party, WP 218, ibid.
[15] Katerina Demetzou, 'GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved' in E Kosta et al (eds), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, vol 547 (Springer International Publishing 2019) 137–54.
[16] GDPR, art 24; Recital 74.
[17] Article 29 Data Protection Working Party, WP 173 (n 13); Quelle (n 9).
[18] Article 29 Data Protection Working Party, WP 218 (n 13).
[19] Demetzou (n 15); Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8 *European Journal of Risk Regulation* 506.

obligations based on the estimated risks of processing so that 'they hit the mark on the ground'.[20]

Second, other obligations are triggered only by risky or high-risk processing; when risk is absent, they remain inactive.[21] For instance, obligations to appoint an EU representative (Art 27(2)), maintain records of processing (Art 30(5)) and inform about data breaches (Arts 33–34) are waived when processing is unlikely to result in risk. Conversely, when processing might result in high risk, Article 35(1) mandates a data protection impact assessment (DPIA), evaluating risks to data subjects' rights and freedoms (Art 35(7)), while Article 36 (1) requires consulting supervisory authorities.

Overall, by forming and triggering controllers' obligations, the GDPR's risk-based approach additionally outlines the ways in which the materialisation of such undesirable outcomes should be prevented, e.g., through DPIAs.[22] A harm-based approach would instead favour an 'ex post, outcome-oriented review' over such 'design' obligations.[23] Harm-based approaches also concentrate on actual damage, whereas risk-based ones consider 'every potential as well as actual adverse effect'.[24]

(ii) Conceptual ambiguities of risk

This prominent role of risk in the GDPR contrasts sharply with the ambiguity surrounding its meaning. Recital 76 suggests assessing risk objectively 'by reference to the nature, scope, context and purposes of the processing'. Lacking a concrete framework, however, this requirement of objective assessment rings hollow. Recital 77 broadly recommends guidance through codes of conduct, certifications and guidelines – yet, the Article 29 Data Protection Working Party (WP29) avoids

[20] Quelle (n 9); Arts 25(1) and 32(1) exemplify this calibration, positing that data protection by design and by default and security measures respectively should rely on the risks incurred by processing.
[21] Macenaite (n 19); Quelle (n 9).
[22] Quelle ibid.
[23] ibid.
[24] Article 29 Data Protection Working Party, WP 218 (n 13).

indicating relevant frameworks.[25] Slightly more concrete guidance is available through examples. Recital 75 associates risk to rights and freedoms with the risk of 'physical, material or non-material damage', including cases where processing might:

- cause discrimination, identity theft, financial loss, reputational damage, loss of confidentiality, reidentification, or other significant economic or social disadvantage;
- obstruct data subjects' rights, freedoms and control over their data;
- concern special categories of personal data;
- lead to profiling that evaluates one's work, economic, health or other situation;
- concern vulnerable natural persons, particularly children; or
- involve numerous personal data and data subjects.

Recital 91 likewise considers risky the processing of special category data and processing that prevents data subjects from exercising rights or using services/contracts. This inductive approach, however, does not yield generalisable criteria for assessing types of risk beyond those mentioned in the examples.[26]

Even these examples, though, are inconclusive. Recital 75 conflates the outcomes of processing (e.g., discrimination) with processing itself (e.g., processing of special category data), obscuring which of the two should be assessed.[27] A way out of this confusion is plausible through the WP29's definition of risk as 'a scenario describing an *event* and its *consequences*, estimated in terms of severity and likelihood'.[28] Macenaite assigns risk to rights and freedoms to the category of *consequences* and

[25] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (WP 248, 4 Apr 2017).
[26] Demetzou (n 15).
[27] This confusion is epitomised in art 35(1), which reads: 'Where a type of processing […] is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact […] on the protection of personal data.' It is, therefore, uncertain whether the object of assessment should be the risk to rights and/or to the protection of personal data. R Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 *Computer Law & Security Review* 279.
[28] Article 29 Data Protection Working Party, WP 248 (n 25). Emphasis added.

protection of personal data to the category of the *event* leading to said consequences.[29] Processing that is risky, meaning non-compliant with data protection law, exposes natural persons to the risk of having their rights violated. Following this interpretation, 'a harm is the violation of a fundamental right stemming from the processing of data as well as the material and moral implication of the latter'.[30] Hence, risk assessment examines compliance of data processing and violations of rights/freedoms in tandem. Nonetheless, most GDPR provisions[31] suggest risk factors about processing itself; only Recital 75 provides risk factors about the violation of rights and freedoms and relevant negative consequences (eg, discrimination).

Often intangible, these negative consequences resist the quantification typically required for risk assessments.[32] Such consequences are varied and subjectively perceived on the basis of individual and collective factors (e.g., experience, age, education, cultural norms and regulations).[33] In light of such variations, exposure to identical risks does not imply identical harm; certain individuals or groups might be more vulnerable to a risk or harm than others.[34] Although Recital 75 mentions vulnerable persons, it does not clarify who (besides children) is considered as such. More helpfully, the WP29 interprets vulnerability as a power imbalance between data subjects and controllers.[35] Hence, far from being objective or quantifiable, risk is individualised and relational, casting doubts on the GDPR's abstract risk-based approach and its suitability for addressing distinct vulnerabilities.[36]

In addition, although the GDPR is technologically neutral, its risk-based approach is not immune to contextual, including technological, change.[37] On a broader level,

[29] Macenaite (n 19).
[30] Gellert (n 27) 282.
[31] For example, GDPR art 35(3) and Recital 83.
[32] Macenaite (n 19).
[33] ibid.
[34] Gianclaudio Malgieri, *Vulnerability and Data Protection Law* (Oxford University Press, 2023).
[35] The examples offered by the WP 29 are more diverse than the GDPR's, encompassing children, employees, those suffering from illnesses, asylum seekers, older people, and generally cases warranting special protection. Article 29 Data Protection Working Party, WP 248 (n 25).
[36] Macenaite (n 19).
[37] Demetzou (n 15).

emerging technologies exhibit considerable complexity and autonomy, while processing and generating large volumes of data.[38] They introduce new or amplify existing risks. They likewise reveal new vulnerabilities as well as dimensions of rights and freedoms.[39] Key among the latter is the collective dimension of privacy, since data-driven technologies pose risks to not only individuals but also groups and society at large.[40] The GDPR's inclusion of such risks is not straightforward, leading to calls for the recognition of 'interdependent privacy' or 'group privacy rights'.[41] On a more specific level, risk changes within a single data processing activity, when its components (e.g., supporting factors) or context (e.g., purpose) evolve.[42] The latter also involves changes in the wider organisational or societal context of the processing activity—for instance, if 'new categories of natural persons become vulnerable to discrimination'.[43] To account for these changes, risk needs a dynamic interpretation; this might, however, add to the obscurity of the risk-based approach.

This obscurity is exacerbated in terms of the subject(s) to whom risk refers. The WP29 excludes controllers' legitimate interests from the assessment: the risks of interest are those posed to individuals rather than the organisation performing the data processing (as happens with risk-based approaches in other fields).[44] Most risk-related provisions also mention natural persons instead of data subjects, encompassing individuals beyond those whose data are being processed.[45] This choice is welcome,

[38] ibid.
[39] ibid; Article 29 Data Protection Working Party, WP 248 (n 25).
[40] Demetzou (n 15); Macenaite (n 19).
[41] Demetzou, ibid. A useful analysis of this dimension comes from Bieker, who refers to the 'duality of data protection law', including both an individual and a structural aspect, with the latter postulating requirements for the organisation of public and private entities when processing personal data, thereby encompassing holistic considerations of risk and power dynamics. He also argues for the *de lege ferenda* recognition of collective rights, especially of minorities or other vulnerable groups, through an extension of the term 'data subject' such that it would allow the enforcement of data subject rights by groups: F Bieker, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law* (TMC Asser Press, 2022).
[42] Article 29 Data Protection Working Party, WP 248 (n 25).
[43] ibid.
[44] Article 29 Data Protection Working Party, WP 218 (n 13); Article 29 Data Protection Working Party, WP 248 (n 25).
[45] See, eg, arts 24(1), 25(1), 27(2), 32(1), 33(1), 34(1) and 35(1).

given that data-driven technologies affect more individuals than the ones linked to the input data (eg, through profiling).

Nevertheless, exactly whose risk is considered remains unclear. Individual subjects and processing activities are certainly included but the inclusion of collective subjects and processing is blurry. Although Recital 75 mentions 'significant social disadvantage' and 'processing that concerns numerous data subjects', these non-binding references appear to denote merely considerations of scale; their application to more structural risks or technological and business practices is questionable. At the other end, the WP29 holds that risk assessments should range 'from an impact on the person concerned by the processing in question to a general societal impact (eg, loss of social trust)', which is too broad to reliably guide controllers.[46]

(iii) Tension between risks and rights

This risk-based approach co-exists with a conventional rights-based one, safeguarding data subject rights in Chapter III of the GDPR and the right to personal data protection throughout the text. This co-existence of risks and rights—especially as a 'risk to a right'—is challenging. In particular, the scalability of accountability obligations challenges the traditional rights-based approach. According to the latter, the right to data protection, as an EU fundamental right, should be upheld in a uniform manner, not based on risk.[47]

The same applies to data subject rights (eg, access, rectification, erasure, objection, transparency, right to be forgotten, right to data portability), which lack the scalability inherent in the risk-based approach. The right of access (Article 15), for instance, is absolute.[48] Controllers should take measures to fulfil this right when it is exercised—eg, through documentation.[49] However, it is unclear whether the right of access

[46] Article 29 Data Protection Working Party, WP 218 (n 13).
[47] Quelle (n 9).
[48] ibid.
[49] ibid.

should be upheld regardless of the risk level (following the rights-based approach) or whether documentation obligations should be proportional to the risk level, allowing limited access rights in cases of low-risk processing (following the risk-based approach).

To address this ambiguity, the WP29 argued that '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'.[50] It stressed that the risk-based approach should not compromise data subjects' rights; these should be respected to the same extent regardless of the risk of the processing examined.[51] The WP29 thus confined scalability to controllers' compliance in the context of the risk-based approach.[52] That the two approaches are distinct does not, however, mean that they are unrelated. As mentioned above, risk assessment examines compliant data processing *and* consequences on rights and freedoms, with higher/lower compliance leading to respectively higher/lower protection of rights. In that sense, the risk-based approach could foster rather than oppose the rights-based one.

The relation between the two approaches is further complicated by the rights pertinent to the risk-based approach. Although data subjects' rights and the right to data protection are expressly mentioned, the articulation of risk-related provisions suggests a broader scope. Recital 75 mentions 'risk to the rights and freedoms of natural persons' in general and offers varied examples of these, while Article 35(1) adopts the same phrasing. The WP29 elucidates that references to rights and freedoms imply 'the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.'[53] Nevertheless, as with the

[50] Article 29 Data Protection Working Party, WP 218 (n 13).
[51] ibid.
[52] As the WP29 stated, 'a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk' ibid.
[53] ibid.

risk factors and examples of Recital 75, this indicative enumeration of rights fails to consistently guide the implementation of the risk-based approach.

Even worse, there is no guidance about the possibility of negative consequences (ie, violation of rights) without an event (ie, non-compliant processing). A data processing activity might incur risks to natural persons' rights and freedoms despite appearing compliant, in the sense of following 'a reasonable and foreseeable interpretation of the rules and principles'.[54] Article 36(1) empowers supervisory authorities to take action against the intended data processing if they consider that 'the controller has insufficiently identified or mitigated the risk' but under the condition that the processing does not comply with the GDPR.

Similarly, the WP29 acknowledges authorities' role in 'carrying out enforcement procedures in case of non-compliance of controllers, which may imply challenging risk analysis, impact assessments as well as any other measures carried out by data controllers'.[55] There is no acknowledgement, however, of the case in which data processing is superficially compliant—or at least cannot be promptly affirmed as non-compliant—yet still exposes natural persons to risk.[56] This omission is important, as the GDPR does not provide for an independent, general obligation to protect natural persons against risks to their rights and freedoms; such an obligation instead exists only in the context of implementing other GDPR provisions.

(iv) Over-reliance on controllers

The ambiguity surrounding risk entails that its identification and management are left to the controllers' discretion. The role of interpreting the relevant provisions and implementing appropriate responses, a role hitherto confined to public entities, is now delegated to a private one.[57] Hence, this reliance on controllers departs from risk-

[54] Quelle (n 9).
[55] Article 29 Data Protection Working Party, WP 218 (n 13).
[56] Quelle (n 9).
[57] Gonçalves (n 11).

based regulation as an approach commonly employed by governments and regulatory agencies.[58] This departure is not absolute, since supervisory authorities can challenge controllers' risk assessment and measures or adopt a risk-based approach to their own activities. Nonetheless, one might wonder whether the GDPR places 'unjustified faith in self-regulatory enforcement of data protection rules' and, relatedly, whether controllers are well placed to undertake these risk assessments.[59] In particular, risk assessments should consider negative consequences that might be intangible (eg, significant social disadvantage), subjective (ie, dependent on one's risk perception) or related to values and norms (eg, discrimination). These aspects render risk contestable and difficult to anticipate or objectively measure. This difficulty is aggravated by controllers' flexibility in using risk assessment frameworks of their choice, raising further uncertainty about the level of data protection across the EU and controllers' liability for these methodological choices.[60]

Instead, the experience and views of those affected by data processing do not factor into the risk assessment. Pursuant to Article 35(9) on DPIAs, '[w]here appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations'. With the appropriateness of such consultation being entrusted to the controllers' interpretation, this obligation remains soft and far-fetched. Drawing on the exemption of commercial interests, private entities are likely to refrain from sharing details about their processing activities for the—actual or ostensible—purpose of safeguarding commercially sensitive information and retaining competitive advantages. [61]

Conversely, the articulation of risks by 'those who live with them and experience them' would benefit risk assessment and management.[62] Input by affected individuals

[58] Macenaite (n 19).
[59] ibid.
[60] ibid; Article 29 Data Protection Working Party, WP 248 (n 25).
[61] Macenaite (n 19).
[62] Niels van Dijk, R Gellert and K Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 *Computer Law & Security Review* 286.

would have two benefits; it would help controllers identify risks that might not be obvious as well as understand individuals' concerns and risk perceptions,[63] and it would help these individuals become aware of how their data are processed, thereby enhancing transparency and trust.[64] Even when data subjects are consulted, the provision does not require that their input is taken into account or that it feeds into measures to be adopted.[65] Equally, there are no provisions on whom such a consultation should involve and what procedures it should follow.[66] WP29's only guidance is that the controller's reasons for deviating from data subjects' input or avoiding to consult them in the first place should be documented.[67] Although the possibility of public engagement in principle exists under the GDPR, it regrettably remains 'of an informational nature and neither provides assurances of comprehensive risk identification nor guarantees a full-pledged protection from risks'. [68]

III. Gendered risks and the GDPR

As Part II illustrated, EU data protection law is undergoing a 'riskification'- understood as a 'move out from the limited boundaries of formal legality of processing of data and enforcement of individual rights against companies' and 'towards a model of "enforced self-regulation" for managing technological innovation in uncertain scenarios'.[69] This riskification occurs in overly broad and ambiguous ways. More importantly, this riskification has not bothered to concern itself with the fundamental question: *whose* data protection risks matter within the GDPR?[70] Does the EU data protection law account for risks that are currently invisible in the GDPR?

[63] Macenaite (n 19).
[64] ibid.
[65] ibid.
[66] van Dijk, Gellert and Rommetveit (n 62).
[67] Article 29 Data Protection Working Party, WP 248 (n 25).
[68] Macenaite (n 19) at 531.
[69] Alessandro Spina, 'A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics' (2017) 8 *European Journal of Risk Regulation* 89.
[70] As Tzanou has put it, 'Data protection *for whom*?' See, Tzanou (n 4) at 454.

The following section takes a closer look at what we argue has been overlooked by the GDPR's risk-based approach, *gendered* risks, and discusses why they matter.

(i) Surveillance of women and femtech

Women have, throughout history, experienced diminished levels of privacy as their bodies have been treated as 'property' of their fathers, husbands or men in general.[71] Privacy, as a right, has functioned as a double-edged sword for women, and popular conceptions of privacy have been criticised by prominent feminists as providing 'a shield for domestic violence'.[72]

Modern technologies have intensified the surveillance of women by providing 'almost limitless ways to harass and control' them.[73] As the UN Special Rapporteur on the Right to Privacy has observed, 'women can expect that nearly every detail of their intimate lives will be subject to multiple forms of surveillance by State as well as private actors, from domestic violence to sexual objectification and reproduction'.[74] Women must navigate 'hidden cameras, the possibility of recorded sexual assaults, threats of "revenge porn", … the proliferation of online mobs engaging in vicious campaigns of sustained sexualised abuse',[75] deepfakes,[76] cyberflashing,[77] and so on.[78] Technologically facilitated gender-based violence 'combines issues of gender inequality, sexualised violence, internet regulation, internet anonymity, and privacy'.[79]

---

[71] See Reva Siegel, '"The Rule of Love": Wife Beating as Prerogative and Privacy' (1996) 105 *Yale Law Journal* 2117; Michelle J Anderson, 'Marital Immunity, Intimate Relationships, and Improper Inferences: A New Law on Sexual Offences by Intimates' (2003) 54 *Hastings Law Journal* 1465.

[72] Catherine MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1991) 193; Elizabeth Schneider, 'The Violence of Privacy' (1991) 23 *Connecticut Law Review* 973.

[73] Human Rights Council, 'Report of the Special Rapporteur on the Right to Privacy' (A/HRC/40/63, 27 February 2019) para 72.

[74] ibid, para 81.

[75] Mary Anne Franks, 'Democratic Surveillance' (2017) 30 *Harvard Journal of Law & Technology* 425, 447.

[76] Mary Anne Franks and Ari Ezra Waldman, 'Sex, Lies and Videotape: Deep Fakes and Free Speech Delusions' (2019) 78 *Maryland Law Review* 892.

[77] Lewis Adams, 'Cyber-flashing convict is first to be jailed under new law' *BBC News* (London, 19 March 2024). Available at: www.bbc.co.uk/news/uk-england-essex-68543605.

[78] Ian Sample, 'Internet "Is Not Working for Women and Girls", says Berners-Lee' *The Guardian* (London, 12 March 2020). Available at: www.theguardian.com/global/2020/mar/12/internet-not-working-women-girls-tim-berners-lee; Human Rights Council 2019, A/HRC/40/63 (n 73), para 78.

[79] Human Rights Council 2019, A/HRC/40/63 (n 73), para 72.

A range of different actors are involved in the surveillance of women: from the market and private entities (such as employers, insurance companies, healthcare providers, advertisers) to intimate partners and ultimately governments.

Femtech has emerged as a new form of surveillance of women's bodies, health and reproductive choices and intimate relations. 'Femtech', a term coined by Ida Tin, the co-founder of menstrual tracking app Clue, refers to a multi-billion-dollar technology industry that offers a variety of technological tools to monitor and manage women's sexual and reproductive health and wellbeing.[80] It encompasses a broad range of software (apps) and hardware (wearables) aimed at supporting women and gender minorities to track, understand and manage their menstrual, reproductive and sexual health. Femtech apps track a range of different aspects of women's sexual and reproductive health, such as menstruation,[81] fertility[82] and menopause symptoms.[83] Data users input, for example, about flow rate is then used to make predictions about future experience (i.e. fertility windows and the start date of future menstrual cycles)[84] or to offer 'personalised' information about menstrual/reproductive health and symptom management.[85]

Femtech wearable devices are worn on the body and use sensors to gather information, such as breast milk production,[86] pelvic floor muscle movements,[87]

[80] 'Femtech' also includes tools geared towards those working within the healthcare system (such as applications which improve screening for breast and ovarian cancer).
[81] Flo Health Ltd UK, 'Flo Period & Cycle Tracker, Apple App Store' (Version 9.41). Available at: apps.apple.com/gb/app/flo-period-cycles-tracker/id1038369065.
[82] FEMOMETER Ltd, 'Femometer – Fertility Tracker, Apple App Store' (Version 5.33.1). Available at: apps.apple.com/gb/app/femometer-fertility-tracker/id1529565125.
[83] Vira Health Ltd, 'Stella | Menopause Relief, Apple App Store' (Version 2.2.2). Available at: apps.apple.com/gb/app/stella-menopause-relief/id1577904186.
[84] Sarah Johnson, Lorrae Marriott and Michael Zinaman, 'Can Apps and Calendar Methods Predict Ovulation with Accuracy?' (2018) 34 *Current Medical Research and Opinion* 1587, 1587.
[85] See, eg, Kristin Mallon, 'Menopause Made Easier: How Femtech Can Transform Symptom Management' (*FemTech World,* 9 June 2023). Available at: www.femtechworld.co.uk/menopause/menopause-made-easier-how-femtech-can-transform-symptom-management/.
[86] Elvie, 'Elvie Trainer'. Available at: www.elvie.com/en-gb/shop/elvie-trainer.
[87] Elvie, 'Elvie Pump'. Available at: www.elvie.com/en-gb/shop/elvie-pump.

changes to cervical fluid,[88] basal body temperature[89] and sleep patterns.[90] Using a connected app, wearables provide information or direct 'bio-feedback'; for example, smart pelvic floor trainers often use vibration to guide the user's exercises.[91] Finally, femtech also encompasses smart sex toys designed for use by women, such as smart vibrators[92] and smart dildos.[93] Many smart sextech are able to be remotely controlled, while some collect biometric data from the user.[94]

To understand the use and popularity of femtech apps and devices, it is necessary to situate these within the broader social and medical context within which they exist (and were developed). There is a recognised tendency to question whether women are trustworthy narrators of their own health and pain,[95] particularly regarding conditions related to the (dis)functioning of the womb.[96] Those experiencing gynaecological symptoms are often 'not listened to'[97] and can face a 'battle' for diagnosis and treatment.[98] There are also substantial knowledge gaps regarding the ways that different gynaecological conditions manifest, as women's health remains under-researched.[99] Sexual, obstetric, post-partum and gynaecological health services

[88] kegg, 'The Science Behind kegg. Available at: kegg.tech/pages/science-behind-kegg.
[89] Tempdrop, 'Tempdrop: Monitor Your Fertility' Available at: www.tempdrop.com/en-gb.
[90] Oura, 'Oura Ring'. Available at: www.ouraring.com.
[91] See, eg, Intima, 'KegelSmart™'. Available at: www.intimina.com/kegel-smart; Elvie (n 85).
[92] Lioness, 'Products: Lioness Smart Vibrator'. Available at: www.lioness.io/products/the-lioness-vibrator.
[93] Lovense, 'Products: Gravity'. Available at: www.lovense.com/thrusting-vibrating-dildo.
[94] The Lioness Smart Vibrator, for example, collects information about the rhythm of pelvic floor movements during use to provide information about arousal and orgasm. Lioness, 'How it Works'. Available at: www.lioness.io/pages/how-it-works.
[95] Anna Nelson, 'Medical Records and Epistemic Injustice: A Women's Health Issue Worthy of Greater Attention' (*APA Blog,* 11 Sept 2023). Available at: www.blog.apaonline.org/2023/09/11/medical-records-and-epistemic-injustice-a-womens-health-issue-worthy-of-greater-attention/.
[96] See, eg, Stella Villarmea, 'When a Uterus Enters the Room, Reason Goes out the Window' in C Pickles and J Herring (eds), *Women's Birthing Bodies and the Law: Unauthorised Intimate Examinations, Power and Vulnerability* (Hart 2020), 70–73; Elinor Cleghorn, *Unwell Women: A Journey Through Medicine And Myth in a Man-Made World* (Weidenfield and Nicolson 2021).
[97] Department for Health and Social Care, *Women's Health Strategy for England* (CP736, Her Majesty's Stationery Office 2022), 7.
[98] All Party Parliamentary Group on Endometriosis 'Inquiry Report; Endometriosis in the UK: Time for Change' (2020) 27.
[99] Department for Health and Social Care (n 97), 2, 6: though note there are ongoing attempts to improve the situation.

are often under-resourced and subject to austerity measures,[100] struggling to meet patients' needs within an appropriate time frame or with satisfactory quality.[101]

Against this backdrop, women often feel that they have to turn to femtech to fill the gaps left by traditional healthcare services. While the current state of women's healthcare operates as a 'push' factor in the femtech context, the marketing of femtech apps and wearables provides a complimentary 'pull' factor. Much of this marketing centres upon a (highly critiqued and contested)[102] promise to 'empower' women and gender diverse users with knowledge about their own sexual and reproductive health, a promise which may resonate well in light of the frustrating lack of appropriate healthcare.[103] Indeed, a number of femtech apps explicitly capitalise upon this gap, positioning their role as spotlighting existing problems, and contributing towards solving these.[104] For example, Flo (a popular menstrual tracking app) observed in its 2023 'Menstrual and Reproductive Misinformation' report that women are struggling to access reliable 'information and support around menstrual and reproductive health', concluding that 'Flo purports to actively helping to close the medical research

[100] Daniela Alaattinoğlu, 'Rethinking Explicit Consent and Intimate Data: The Case of Menstruapps' (2022) 30 *Feminist Legal Studies* 157, 161.

[101] For example, in its 2022 report, the UK Royal College of Obstetricians and Gynaecologists noted that more than half a million women (570,000) were on waiting lists for gynaecological appointments across the UK, and that more than one in 20 patients in England had to wait more than a year for treatment – often for conditions such as endometriosis which have debilitating symptoms. See D Khanna, 'Women's health: Why is the health of at least half the global population so often overlooked?' (*World Economic Forum,* 2 Jan 2022). Available at: www.weforum.org/agenda/2023/01/women-health-gap-davos-2023/; L Hoctor et al, 'Women's sexual and reproductive health and rights in Europe: Issue Paper' (*Council of Europe Commissioner for Human Rights,* December 2017); Royal College of Obstetricians & Gynaecology, 'Left for too long: understanding the scale and impact of gynaecology waiting lists' (nd). Available at: www.rcog.shorthandstories.com/lefttoolong/index.html; Elvie and Motherly, *The Motherload - The Weight of Limited Postpartum Support* (2024).

[102] Michele Estrin Gilman, 'Periods for Profit and the Rise of Menstrual Surveillance' (2021) 41 *Colombia Journal of Gender and Law* 100; Maria Novotny and Les Hutchinson, 'Data Our Bodies Tell: Towards Critical Feminist Action in Fertility and Period Tracking Applications' (2019) 28 T*echnical Communication Quarterly* 332; Tereza Hendl and B Jansky, 'Tales of Self-empowerment through Digital Health Technologies: A Closer Look at "Femtech"' (2022) 80 *Review of Social Economy* 29.

[103] NIHR Evidence, 'Women's Health: Why do Women Feel Unheard?' (Health and Social Care Research, 23 November 2023).

[104] See, eg: Sorina Mihaila, 'Women's pain still not taken seriously, says Clue CEO' (*FemTech World,* 19 Jan 2024). Available at: www.femtechworld.co.uk/news/womens-pain-is-still-not-taken-seriously-says-clue-ceo/.4.

gender gap and producing medically credible content to help inform millions of women.'[105]

While femtech's promise of empowerment for managing sexual and reproductive health is appealing, questions arise about the new ways of controlling women. As observed by Lupton:

> These devices could … be regarded as disciplinary, working to tame the sexual and reproductive body by rendering it amenable to monitoring, tracking, and detailed analysis of the data thus generated …[106]

Women, their bodies, cycles, communications, relationships and activities are constructed as 'monitored subjects'[107] that can be seduced, coerced, disciplined and controlled.[108]

Some femtech products offer an embedded functionality that sends women's period data and other intimate information to partners.[109] Intimate partner surveillance (IPS) often concerns women's sexual and reproductive autonomy issues. IPS that can also be perpetrated through general social media can cause both emotional and physical harm.[110] In the most extreme cases it can lead to violence, including reproductive coercion (which can be perpetrated through femtech) physical assault and even

[105] Flo 'Mind the gaps: Menstrual and reproductive misinformation in the UK in 2023' (2023). Available at: www.flo.health/landings/reproductive-health-report-uk.
[106] Deborah Lupton, 'Quantified Sex: A Critical Analysis of Sexual and Reproductive Self-Tracking Using Apps' (2014) 17 *Culture, Health & Sexuality* 440.
[107] Karen Levy, 'Intimate Surveillance' (2015) 51 *Idaho Law Review* 679, 688.
[108] Rob Kitchin, 'Thinking Critically About and Researching Algorithms' (2017) 20 *Information, Communication & Society* 14, 19.
[109] Sorina Mihaila, 'Period tracking app Flo launches feature for male partners' (*FemTech World*, 20 Oct 2023). Available at: www.femtechworld.co.uk/news/period-tracking-app-flo-launches-feature-for-male-partners/.
[110] Molly Dragiewicz et al, 'Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms' (2018) 18 *Feminist Media Studies* 609.

murder.[111] IPS and domestic violence disproportionately affect women. Official reports indicate that, in 2021, '720 women were murdered by an intimate partner, family member or relative in 17 EU Member States'.[112]

Whether femtech data processing complies with the GDPR is at least debatable.[113] Concerns have been raised with regard to, inter alia, data minimisation, transparency and the appropriate legal bases for processing of such sensitive data, including consent.[114] Indeed, against the current socio-medical landscape, the processing of personal data through femtech apps has been labelled as a 'coercive exchange' – one is required to consent to 'such data collection if one wants to access … services'.[115]

This chapter does not focus on femtech's compliance with the GDPR. Instead, we are interested in investigating the role of the GDPR itself in addressing gendered risks and harms[116] (arising from femtech processing and beyond). What are the potential gendered risks of processing and how could our understanding of risk under the GDPR evolve to encompass gendered risks? Can the GDPR address risks that go beyond individual rights and are embodied, collective and systemic?

Before we attempt to answer these questions, we explain why gender matters within the GDPR.

---

[111] R Chatterjee et al, 'The Spyware Used in Intimate Partner Violence' (2018) *IEEE Symposium on Security and Privacy* 441.

[112] There is currently a lack of comprehensive data regarding gender-based violence in the EU. See: European Institute for Gender Equality 'Gender Equality Index. Domain: Violence in the European Union (2023)'. Available at: www.eige.europa.eu/gender-equality-index/2023/domain/violence. More comprehensive data is expected to be published some time in 2024.

[113] See Anastasia Siapka and Elisabetta Biasin, 'Bleeding Data: The Case of Fertility and Menstruation Tracking Apps' (2021) 10 *Internet Policy Review* 4, 5–11.

[114] Alaattinoğlu (n 100).

[115] Renee Shelby, Jenna Imad Harb and Kathryn Henne 'Whiteness In And Through Data Protection: An Intersectional Approach to Anti-Violence Apps and #MeToo Bots' (2021) 10 *Internet Policy Review* 1, 17.

[116] Broadly speaking, the distinction between risk and harm can be understood as follows: A risk can exist without the outcome actually materialising. A harm, however, is definite in character and generally requires a completed action. Adriana Placani, 'When the Risk of Harm Harms' (2017) 36 *Law and Philosophy* 77, 82.

(ii) The GDPR and (the absence of) gender: Women's sexual and reproductive rights and why gender *matters* in data protection law

While technology-facilitated surveillance is gendered, the GDPR – and European data protection law in general - is gender blind.[117] Indeed, neither 'gender' nor 'sex' are mentioned anywhere in the GDPR.[118] Article 9 of the GDPR, which deals with the processing of 'special categories' or 'sensitive data' and establishes an in-principle prohibition of processing of such data because there is a risk that this might lead to, *among others,* discrimination, includes personal data

> revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation,

It, however, does not mention 'gender' ('gender identity') or 'sex'.

This appears a significant oversight in light of Article 21(1) of the EU Charter of Fundamental Rights (EUCFR), which provides that 'any discrimination based on any ground such as *sex*, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited'.[119]

[117] Malgieri and González Fuster (n 5).
[118] Sex is often used to describe the biological characteristics of a person, whereas gender relates to a person's identity – and is increasingly recognised as being socially and culturally constructed. This approach to understanding the sex/gender distinction is one which has been reflected in both international human rights law and European equality law: European Institute for Gender Equality, 'The EU's Evolving Legal and Policy Approaches to Gender Equality' (*Publications Office of the European Union,* 2022), 11; Damien A Gonzalez-Salzberg, 'The Accepted Transsexual and the Absent Transgender: A Queer Reading of the Regulation of Sex/Gender by the European Court of Human Rights' (2014) 29 *American University International Law Review* 797. However, there is also a prominent body of critical scholarship which aims to unsettle the sex/gender binary: eg, Judith Butler, *Gender Trouble* (Routledge 1990); Catherine Clune-Taylor, 'Is Sex Socially Constructed?' in Sharon Crasnow and Kristen Intemann (eds), *The Routledge Handbook of Feminist Philosophy of Science* (Routledge 2020).
[119] Emphasis added.

Remarkably, 'sex' which is a protected characteristic of primary EU anti-discrimination law has not found its way into (or has been (un)consciously excluded from) the provision of the GDPR which aims to address discrimination. The remainder of the text of the GDPR is equally silent on gender (or sex).[120]

The GDPR's gender blindness is not innocuous; it reveals a further significant omission: a lack of acknowledgment of the significance of data protection rights for the safeguarding of women's sexual and reproductive wellbeing and autonomy (which constitutes another gendered problem). As the femtech case study above demonstrates, technology-facilitated gendered surveillance and gendered outcomes are inextricably linked with the sexual and reproductive rights of women and girls (or the lack thereof). According to the UN Working Group on Discrimination Against Women and Girls, 'the full enjoyment of sexual and reproductive health rights is indispensable to the ability of women and girls to exercise all other human rights'[121] and the non-enjoyment of these rights is 'a significant impediment to gender equality, resulting from the persistent failure of States to adequately respect, protect and fulfil those rights'.[122]

As the Council of Europe Commissioner has also observed, without 'effective state action to guarantee sexual and reproductive health and rights … some of the most significant and intimate aspects of our lives as human beings are at risk'.[123] Indeed, there cannot be gender equality without reproductive autonomy.[124] Alongside reproductive rights and autonomy, sexual rights have been recognised not only as

[120] 'Sex life' is mentioned in Recital 75 and 'sexual orientation' in Recital 71.
[121] Human Rights Council 'Women's and Girls' Sexual and Reproductive Health Rights in Crisis: Report of the Working Group on Discrimination Against Women and Girls' (A/HRC/47/38, 28 Apr 2021) para 8.
[122] ibid, 1.
[123] Hoctor et al, (n 101) at 5.
[124] See, eg, Carolina Fredrickson, 'Gender Equality Depends on Reproductive Freedom' (*SDG Action,* 2 Mar 2023). Available at: www.sdg-action.org/equality-depends-on-reproductive-rights/; Ranee Thakar, 'Sexual and reproductive health and rights must remain a priority for the UK's agenda for global gender equality' (*RCOG Blog,* 6 March 2023). Available at: www.rcog.org.uk/news/blog-sexual-and-reproductive-health-and-rights-must-remain-a-priority-for-the-uk-s-agenda-for-global-gender-equality/.

'fundamental human rights', but also as 'an essential component for human development' and 'fundamental to individual health and wellbeing'. [125] Yet, there remains substantial stigma attached to women's sexuality, sexual pleasure and sexual expression,[126] which has 'negative implications for women's sexual autonomy, agency and freedom' and their wider wellbeing.

Gender inequality – understood as 'systemic disadvantages for women throughout their life cycle'[127] – is tied to women's sexual and reproductive status. [128] Indeed, women experience a number of 'life milestones'[129] such as menstruating, trying to conceive, giving birth and managing the menopause that make them prone to exploitative market practices seeking to capture and capitalise upon data related to these realities. [130] Women are far more likely to make use of femtech given inequalities in access to healthcare, which increases the gendered disparity of this kind of data extraction. Many women and girls regularly face sexual and reproductive crises, such as period poverty, unplanned pregnancy and sexual violence. [131] These crises are linked to 'structural discrimination and fostered by the patriarchal oppression, pervasive gender stereotypes, stigma and taboos that drive gender inequality'.[132] Finally, 'in a context of rising fundamentalisms, backlash against gains in women's equality' once again 'target sexual and reproductive health rights'.[133] Many of the

[125] Jessie V Ford et al, 'Why Pleasure Matters: Its Global Relevance for Sexual Health, Sexual Rights and Wellbeing' (2019) 31 *International Journal of Sexual Health* 217, 218.
[126] Hoctor et al (n 101) at 26.
[127] Human Rights Council 2021, A/HRC/47/38 (n 121), para 12.
[128] ibid.
[129] Lucy Purdon, 'Unfinished Business: Incorporating a Gender Perspective into Digital Advertising Reform in the UK and EU' (*Mozilla Foundation*, October 2023), 11.
[130] Danielle Keats Citron has noted that women are 75% more likely to use health apps than men: *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (Chatto & Windus 2023) 14–15.
[131] As the UN notes 'an estimated 810 maternal deaths occur each day globally, 15 and 25 million unsafe abortions take place annually, resulting in approximately 47,000 deaths every year, primarily in developing countries and among members of socioeconomically disadvantaged and marginalized populations. Every 16 seconds there is a stillbirth. More than 200 million women who want to avoid pregnancy are not using modern contraception, due to a range of barriers. Millions of women and girls are denied the ability to manage their monthly menstrual cycle safely and with dignity'. Human Rights Council 2021, A/HRC/47/38 (n 122) at para 16.
[132] 'Human Rights Council 2021 (n 121) at para 12.
[133] ibid para 17.

issues that women and girls face in relation to their sexual and reproductive autonomy 'can be ascribed to the instrumentalization and politicization of their bodies'. [134]

Achieving sexual and reproductive justice requires dealing with large, systemic and deeply rooted social ills such as discrimination, poverty, gendered, racial and socio-economic subjugation, and their multiple and complex underlying causes. It would require making the agency and autonomy of women and girls central to all sexual and reproductive health laws and policies.[135]

This chapter undertakes a more modest task: it argues that data protection and privacy have a significant role to play when the sexual and reproductive health rights of women and girls are at risk.[136] Indeed, gender *matters* for the enjoyment of the privacy and data protection rights of women.[137] As discussed above, femtech is a form of self-participatory surveillance, where women 'willingly' give information related to their reproductive and sexual activity to apps and wearables (primarily) created by private entities for profit. However, what makes the femtech case study important is that it lies at the intersection of data protection and reproductive rights,[138] and provides useful context on how digital products which process intimate personal data – with consent – might affect women's reproductive rights, autonomy and decision making.

Data protection (and privacy) are 'essential to the free development of individuals personality and identity', serve as 'necessary preconditions for the protection of fundamental values, such as dignity, liberty and equality', and 'facilitate the exercise and enjoyment of other human rights',[139] including bodily integrity and sexual and

[134] ibid.
[135] ibid.
[136] This issue goes beyond 'decisional privacy' as understood in the US context. It concerns data protection as understood in the EU context.
[137] As well as trans and gender diverse individuals. See, eg, Cayce C Hughes, 'Not Out in the Field: Studying Privacy and Disclosure as an Invisible (Trans) Man' in D'Lane R Compton, Tey Meadow and Kristen Schilt (eds), *Other, Please Specify* (University of California Press 2018) 111–25; Toby Beauchamp, *Going Stealth: Transgender Politics and U.S. Surveillance Practices* (Duke University 2019).
[138] See Katie Krumbholz, Alice Militaru and Kyle J Morgan, 'Tracking the Trackers: 'Menstruapp' Privacy Policies Following the Dobbs Decision' (2024) 45 *Journal of Women, Politics & Policy* 167.
[139] Human Rights Council 2019, A/HRC/40/63, (n 73) at para 52.

reproductive autonomy. As digital technologies make it increasingly difficult to distinguish (gendered) 'bodies' from their (gendered) 'data doubles' in the information society,[140] the femtech case study demonstrates that data protection – and the GDPR – is integral to the realisation of sexual and reproductive rights which are 'intrinsic to every woman and girl and tied to their ability to live with dignity and exercise their agency'.[141]

Indeed, the UN Special Rapporteur on the Right to Privacy has emphasised that '[g]ender based breaches of privacy are a systemic form of denial of human rights; discriminatory in nature and frequently perpetuate unequal social, economic, cultural and political structures'.[142] In light of this, he stressed that 'gender should be a key consideration for the development and enforcement of privacy protection frameworks',[143] and has called States to develop frameworks to address and prevent gender based privacy invasions, by actively protecting privacy in policy development, legislative reform and regulatory action.[144]

Regrettably, the GDPR, through its gender-blind approach, fails to recognise that personal data (and data gaps), data subjects[145] and risks of processing – which constitutes the focus of the present chapter – can be *gendered*. Admittedly, sexual and reproductive data could be considered 'data concerning health'[146] and, thus, fall within the special categories of data under Article 9 of the GDPR. However, this is not sufficient; it misses out that such data and more importantly their processing might entail gendered risks associated with sexual and reproductive rights, which are intrinsic to every woman and girl. The lack of any mention of gender renders any potential link between health data and women's sexual and reproductive rights too

[140] Kevin D Haggerty and Richard Ericson, 'The Surveillant Assemblage' (2000) 51 *The British Journal of Sociology* 605.
[141] Human Rights Council 2021, A/HRC/47/38 (n 121) para 71.
[142] Human Rights Council 2019, A/HRC/40/63 (n 73) para 104.
[143] ibid.
[144] ibid para 106.
[145] Malgieri and González Fuster (n 5).
[146] These are defined in GDPR art 4(15) as 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'.

weak. These are viewed as 'sensitive data' to the extent that they are regarded as data concerning health, but they lack a recognition of their gendered significance to women and girls.

This reveals a gap in the GDPR: symbolically, the potential gendered impact of processing is not sufficiently important to even be mentioned among the numerous GDPR recitals with the concomitant normative consequences of effacing any relevant legal recognition (for half of the population). The EU legislator's choice to refrain from any mention of gender (or even to the less preferable term 'sex') is 'particularly striking'[147] in light of its significance in relation to personal data processing (although, admittedly, this is not unique to data protection law).[148]

IV. Re-imagining the GDPR: A gender responsive approach

In light of the above analysis, we argue that the GDPR should be(come) gender responsive. This entails a core normative argument calling for a reimagination of the GDPR so that it considers the 'gendered realities' of the society we live in and ensures that 'injustices are not replicated as we race towards digital development'.[149] This proposal continues Tzanou's work on the egalitarian 'reconstruction' of EU data protection law so that this can address substantive justice concerns;[150] in light of the recent Feminist Data Protection research, which calls for an interrogation of data protection so that this pursues intersectional feminist objectives;[151] and Malgieri's and Fuster's important work on the gendered 'vulnerable' data subject.[152]

Our contribution advances these debates by focusing on *gendered risks* under the GDPR. The focus on 'gendered risks' is important for two reasons. First, while a risk-based approach is central to the GDPR, the possibility of data processing risks being

[147] Malgieri and González Fuster (n 5).
[148] Gender is seen as 'barely visible in the conceptual armoury of law'. See Joanne Conaghan, *Law and Gender* (OUP 2013) 5.
[149] Sachini Perera, *White Paper on Feminist Internet Research* (Association for Progressive Communications, 2022) 48.
[150] Tzanou (n 4).
[151] Theilen et al (n 4).
[152] Malgieri and González Fuster (n 5).

'gendered' has not been considered so far by the law, the relevant case law, the data protection authorities,[153] or the academic literature surrounding EU data protection law. More importantly, we consider that the risk-based approach can and should bring gender concerns within the scope of the GDPR in light of the gendered surveillance of women's data and bodies currently undertaken by market actors, states and intimate partners. Indeed, these concerns cannot be fully captured by looking merely at potentially gendered personal data,[154] or by considering the (gendered) data subject as 'vulnerable'.[155] A focus on 'gendered risks' provides a more dynamic and flexible approach, which aligns with the GDPR's focus on risks. It also enables a broader understanding of risks than the one currently adopted by the GDPR, which, beyond *individual* ones, encompasses *collective*, *systemic*, *embodied* and *societal* (*gendered*) risks.

(i) Conceptualising *gendered* risks: Definitions and categories

As discussed, despite its centrality to the GDPR, risk is fraught with conceptual ambiguities. This makes the task of conceptualising *gendered* risks challenging. Based on the dimensions of *event* and *consequences*, the GDPR is concerned with risks to natural persons' rights and freedoms arising from personal data processing. This is useful for our discussion: *gendered* risks could be understood 'as risks to the rights and freedoms of natural persons *related to gender* and arising from personal data processing'.[156] This understanding is broad: it includes risks related to gender that might arise from the processing of *gendered personal data*, risks that might arise from

[153] Though the Data Protection Authorities in both Poland and Spain have drawn a potential connection between *vulnerability* and gender in the data protection context: Malgieri and González Fuster, n.5 at 8. The UK ICO has also recognised the potential for specific data protection concerns to arise in the (gendered) context of menstrual trackers and fertility apps: Information Commissioner's Office (ICO), 'ICO to Review Period and Fertility Tracking Apps as Poll Shows More than Half of Women Are Concerned over Data Security' (*Media Centre*, 7 September 2023) ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/09/ico-to-review-period-and-fertility-tracking-apps.

[154] It would be difficult to define these and delineate *in abstracto* why they would require enhanced protection as well as clearly distinguish what should be included or excluded from such an exercise.

[155] Malgieri and González Fuster note that 'vulnerability' – and most generally the very notion of 'protection' – is 'a double-edged sword, not necessarily always benefiting the holder of the label': Malgieri and González Fuster, n.5 at 25.

[156] Emphasis added.

gendered processing and, more generally, risks that relate to gender but arise from what could be considered gender neutral processing of personal data. Our focus here is to the potential or the actual adverse effect of personal data processing *relating to gender*; if such a potential adverse effect exists, we submit that this would be considered a *gendered risk*.

This broad understanding of gendered risks includes different types of risk: *individual*, *embodied*, *collective* and *societal gendered risks*.

a. Gendered individual risks

Our proposed understanding of *gendered risks* captures *individual risks* which constitute the GDPR's focus. Let us take an example from femtech. Assume that a woman uses a fertility and ovulation app to get pregnant and, subsequently, to track her pregnancy. Without the woman's awareness, her data are further shared with third parties, including Facebook and Google, for analytics and marketing purposes.[157] Although such third-party sharing is essential to the business models of several digital technologies, when performed in the femtech context, it predominantly relies on and affects women. As mentioned in III.2, the marketing practices for which this data sharing is employed are gendered, capitalising on data related to reproductive milestones.[158] Such data enable the segmentation of marketing targets into similarly reproduction-related profiles(eg, 'heavy purchaser of pregnancy tests' or 'infertility/IVF').[159]

Based on these data and profiles, marketers make assumptions about women's desires and likely purchases, with the prevalent assumptions being that they desire to conceive or that they will desire baby products nine months after conception.[160] These

[157] This is not a hypothetical example. See Zoe Schiffer, 'Period tracking app settles charges it lied to users about privacy' (*The Verge,* 13 Jan 2021). Available at: www.theverge.com/2021/1/13/22229303/flo-period-tracking-app-privacy-health-data-facebook-google.
[158] Purdon (n 129) above.
[159] ibid.
[160] ibid.

assumptions feed into advertising practices which, unbeknownst to the femtech users on whose data they rely, might be experienced by women as unnecessary and creepy or even shameful and upsetting, depending on their individual circumstances.[161] For instance, being targeted with Facebook ads about unwanted baby products might be highly distressing for a woman who has just suffered a stillbirth.[162] This sharing of the data with third parties without explicit consent impacts the individual and is, therefore, an individual risk/harm[163] that the GDPR recognises. Additionally, we argue that it is also an example of a *gendered individual risk* because it has an individual adverse effect relating to gender -through its inextricable connections to women's reproductive life.

b. Gendered embodied risks

Our understanding of gendered risks further includes *embodied* risks. For example, let us imagine that a woman uses a smart vibrator which is not sufficiently secure and is, therefore, hacked by a third party. Sextech offers women and gender minorities knowledge and control over their sexuality and sexual pleasure, something which has often been denied to them within the patriarchal society. Against this, we submit that the woman in our example has suffered an *embodied gendered* harm. The loss of control over the flow of her intimate data generated through the smart device and accessed by an unwanted third party is an *embodied* harm.[164] As we explain elsewhere,[165] this also gives rise to a further embodied harm understood in the narrow sense: the user's bodily integrity itself is violated since the vibrator is controlled by an unwanted third party (this constitutes a sexual offence type harm).

[161] ibid.
[162] Gillian Brockwell, 'Dear tech companies, I don't want to see pregnancy ads after my child was stillborn' *The Washington Post* (Washington DC, 12 Dec 2018). Available at: www.washingtonpost.com/lifestyle/2018/12/12/dear-tech-companies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn/.
[163] The GDPR does not mention 'harm'. It instead uses 'risk' or 'damage' terminology.
[164] ibid.
[165] ibid.

Embodied risks broadly understood as having an impact on bodily integrity, are not explicitly acknowledged in the GDPR, but we argue that they matter because new technologies and their applications increasingly collapse the boundaries between the data and the body. The body is implicated in the use of online spaces and technologies and both this and bodily subjectivity, are 'central to the experience one has in online spaces'.[166]

Digital embodiment offers a response to 'digital dualism', by situating the body 'as central to the lived experience of digital culture'.[167] Popularised by Jurgenson,[168] the concept of 'digital dualism' refers to 'a bias that treats offline/physical life as real and online/digital life as virtual and somehow less real'.[169] Embodiment in this context implies that the harms experienced in the virtual world can have 'real effects, both bodily and psychical' which are 'not tangential, but increasingly central, to how individuals experience and live their everyday lives'.[170] Thus, we can recognise that online, 'noncontact' offences may give rise to embodied harms[171] in the context of autonomy, dignity or bodily integrity. For instance, survivors of image-based sexual abuse experience the harms of this 'in and through their bodies, altering their sense of bodily integrity, and their corporeal, social and sexual subjectivity'.[172] In the reproductive context, scholars have emphasised the 'experientially profound' nature of pregnancy and birth[173] and highlighted that looking at reproductive issues through

---

[166] Chandell Gosse, '"Not the Real World": Exploring Experienced of Online Harm, Digital Dualism and Ontological Labour' in Jane Bailey, Asher Flynn and Nicola Henry (eds) *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Publishing Ltd 2021) 49.

[167] ibid, 50.

[168] N Jurgenson, 'Digital dualism versus augmented reality' (*The Society Pages: Cyborgology*, 24 Feb 2011). Available at: www. thesocietypages.org/cyborgology/2011/02/24/digital-dualism-versus-augmented-reality/; Nathan Jurgenson, 'Digital dualism and the fallacy of web objectivity' (*The Society Pages: Cyborgology*, 13 Sept 2011). Available at: https://thesocietypages.org/cyborgology/2011/09/13/digital-dualism-and-the-fallacy-of-web-objectivity/; Gosse (n 166), 48.

[169] Gosse, ibid at 48.

[170] Nicola Henry and Anastasia Powell, 'Embodied Harms, Gender, Shame & Technology Facilitated Sexual Violence' (2015) 21 *Violence Against Women* 758, 766; See also, Jennifer Laffier and A Rehman, 'Deepfakes & Harm to Women' (2023) 3 *Journal of Digital Life & Learning* 1, 3.

[171] Gosse (n 166) at 50; Henry and Powell ibid.

[172] Clare McGlynn et al, '"It's Torture for the Soul": The Harms of Image-Based Sexual Abuse' (2021) 30 *Social & Legal Studies* 541, 550.

[173] Susan Bordo, 'Are Mothers People? Reproductive Rights and the Politics of Subjectivity' in Susan Bordo and L Heywood (eds), *Unbearable Weight: Feminism, Western Culture, and the Body* (University of California Press 2003) 94 (original emphasis); See also, Iris Young, 'Pregnant Embodiment: Subjectivity

the lens of embodiment enables research to examine 'power and how inequality operates on and through bodies'.[174] Combining, therefore, understandings of digital and reproductive embodiment serves to underscore the potential for embodied gendered risks that arises from femtech wearables and apps data processing[175] as the data subjects' lived experience is felt through the body.

Therefore, when thinking about embodied risks in the context of femtech, it is important to consider both embodiment per se, and the gendered aspects of embodiment. Femtech wearables are 'embodied computing technologies'[176] – worn in, on, or around the body, and quantify bodily information through computing. They operate through an 'embodied interaction' with the user,[177] as wireless biosensors placed on the device to collect data flows from within the body. The use of smart (intimate) wearables, thus, implies a 'double embodiment' process whereby the technology is embedded in and works through the user's body,[178] and becomes the means through which the user understands and/or experiences the self. For instance, while placing a smart menstrual cup inside their bodies, users not only do the data work but also use the analytics to understand, track, and manage their menstrual life. The 'double embodiment' thus, produces a 'networked body'[179] – where the intimate self is experienced and embodied through an interconnected assemblage of the biological and the digital. The networked body functions through the data flows between three nodes in the assemblage – the body, the device and the mobile app.

---

and Alienation' (1984) 9 *The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine* 45.

[174] Katrina Kimport and Krystale Littlejohn, 'What Are We Forgetting? Sexuality, Sex, and Embodiment in Abortion Research' (2021) 58 *The Journal of Sex Research* 863, 868.

[175] This section on embodiment builds from other research on Femtech Wearables and Embodied Harm, conducted during as part of the project 'FemTech surveillance: Gendered digital harms and regulatory approaches'. For more information see: https://www.sheffield.ac.uk/law/research/centres-and-institutes/sciel/projects/femtech-surveillance-gendered-digital-harms-and-regulatory-approaches.

[176] Isabel Pedersen and Andrew Iliadis, *Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles* (MIT Press 2020).

[177] Paul Dourish, *Where the Action Is: The Foundations of Embodied Interaction* (MIT Press 2001).

[178] Federica Buongiorno, 'Embodiment, Disembodiment and Re-embodiment in the Construction of the Digital Self' (2019) 12 *HUMANA.MENTE Journal of Philosophical Studies* 310.

[179] Isabel Pedersen, 'Will the Body Become a Platform? Body Networks, Datafied Bodies, and AI Futures' in Isabel Pedersen and Andrew Iliadis (eds), *Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles* (MIT Press 2020) 21–47.

These three nodes are interconnected and collectively inform the user's technologically facilitated intimate embodiment.

Overall, we argue that the GDPR should concern itself with *embodied* risks. Emerging technologies, such as wearables, involve contact with the body and, as such, they implicate interests in autonomy and bodily integrity. Crucially, risks to bodily integrity and autonomy are closely linked to human dignity and matter when considering risks under the GDPR.

c. Gendered collective and societal risks

Although it is unclear whether the GDPR's risk-based approach extends beyond the individual, our proposed understanding of gendered risks encompasses *collective* and *societal* risks. *Collective* or *group* harms occur 'when a group – either aligning with a traditional category or an *ad hoc* group – experiences a harm in their capacity as a member of that group eg, a group of workers, local or indigenous community'.[180] *Societal* harms refer to 'harms affecting larger-scale human groups bounded by persistent interaction, normally sharing the same spatial territory, typically subject to the same political authority and dominant cultural expectations, interests, and norms'.[181] Let us take an example from each category. As part of a workplace wellness programme at a company, employees are given free access to an app which has a period and fertility tracking component and also monitors women's menopausal symptoms.[182] Employees who use the app receive additional benefits and rewards

[180] Chris Thomas et al, 'The Case For a Broader Approach to AI Assurance: Addressing "Hidden" Harms in the Development of Artificial Intelligence' (2024) *SRN Electronic Journal* 1, 5; Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017).

[181] Thomas et al, ibid 5; Luciano Floridi, 'Global Information Ethics: The Importance of Being Environmentally Earnest' (2007) 3 *International Journal of Technology and Human Interaction* 1; Nathalie A Smuha, 'Beyond the Individual: Governing AI's Societal Harm' (2021) 10 *Internet Policy Review* 1.

[182] Drew Harwell, 'Is your pregnancy app sharing your intimate data with your boss?' *The Washington Post* (Washington DC, 10 April 2019). Available at: www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/; Filza Siddiqui 'The Birth of Femtech Lays Fertile Grounds for Pregnancy Discrimination in the Workplace' (2024) 62 *Family Court Review* 413

such as reduced health insurance premiums. The employer who has purchased the app for its employees has access to the data generated by the app, supposedly to make appropriate adjustments to the workplace to support employee wellbeing. Over time, it appears that a number of women employees are refused promotions which they would be expected to get or promotions for women are significantly delayed. In fact, the majority of the women who are using the app 'to get pregnant' are not putting themselves forward for a promotion even if they are at the appropriate career stage.

This would be an example of a *gendered collective harm*. It refers to a small grouping of people (here the women employees) of a company and is gendered because it concerns women's sexual and reproductive data and autonomy. While the gendered data use might lead to workplace discrimination and aspects of it would be captured by EU anti-discrimination law,[183] we argue that the GDPR – and data protection law – should care for these problems as well. This is because women employees are disproportionately subjected to a chilling effect of employer surveillance affecting their reproductive autonomy and their consent or the legal basis used for the processing of such data by their employer is not sufficient to account for the power asymmetries in the context of the employment relationship.

Finally, our understanding of gendered risks includes *gendered societal* risks.[184] As explained, these might also be experienced at an individual level, but their effects might have a systemic and cumulative impact on the lived experiences of women in general. Non-consensual intimate images[185] and deepfakes[186] fall in this category of societal gendered harms and are relevant to the GDPR but let us take another example from the femtech context, which concerns participatory self-surveillance. Imagine that

[183] Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast), OJ L 204, 26.7.2006.
[184] See also Bieker (n 41).
[185] Clare McGlynn, Erika Rackley and Ruth Houghton, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' (2017) 25 *Feminist Legal Studies* 25.
[186] Laffier and Rehman (n 170).

a fertility and ovulation app is funded by anti-abortion campaigners.[187] The app is widely used by women and girls in different countries, including in countries that criminalise abortion and require sharing of such data with law enforcement authorities.

This example – which is not entirely imaginary – raises questions that are difficult to capture within the GDPR's regulatory capacity. First, it involves broader issues around consent.[188] While it could be assumed that women have given valid explicit consent for the processing of their intimate personal data by the app under the GDPR, this consent does not cover femtech's business models and actors involved therein which escape the defined categories found in the GDPR (controller/processor). Would consent under the GDPR to process data by this app cover the fact that the app has been funded by anti-abortion campaigners? How is this fact to be captured when it does not form part of standard privacy policies and terms and conditions but was revealed by the media? Is there any violation of the GDPR at all?

More importantly, we argue that a *societal risk* arises when market surveillance of women's sexual and reproductive autonomy is ultimately used by states to control, police and coerce women's data bodies. We consider this an example of a *gendered societal risk*: the state surveillance and control of women's sexual and reproductive bodies is perpetrated through the 'compelled assistance' of private market companies. The GDPR clearly does not focus on such *gendered societal risks*, but we argue that it *should* be concerning itself with these as a matter of substantive justice.[189]

Overall, as the above examples from the femtech case study demonstrate, gendered risks might produce both *tangible harms* and *intangible harms*. *Tangible harms* refer to physical and material as well as non-material/emotional damage arising from the misuse or abuse of users' personal data, embodied injuries, intimate partner

[187] Jessica Glenza, 'Revealed: women's fertility app is funded by anti-abortion campaigners' *The Guardian* (London, 30 May 2019). Available at: www.theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners.
[188] Alaattinoğlu (n 100).
[189] Tzanou (n 4).

surveillance and discrimination and intangible harms relating to the power asymmetries between women and femtech actors, the inhibitive and controlling effects of femtech surveillance and the opacity of femtech's algorithmic predictions. *Intangible harms* can be more indirect,[190] abstract and, therefore, more difficult to determine[191] often lacking an individualistic focus and requiring attention to scale[192] and to both actors involved in femtech surveillance and bodies subject to its incremental everyday techno-management.

In short, this section identified different risks with which the GDPR should be concerned. These are *individual-level* risks (captured by the current focus of the GDPR), but also *embodied*, *collective* and *societal* risks. These categories are not clear cut but may overlap with each other. It might also be that more than one category of risk is present in a particular case: the risk might be individual, embodied and societal. Crucially, the common characteristic of all these identified types of risk is their *gendered* nature (gender is understood here in an *intersectional* way).[193] While we provided a definition of *gendered risks,* we still need to explain why it is important to identify risks as gendered under the GDPR and, more broadly, in EU data protection law. We now turn to this question.

(ii) Why should the GDPR recognise gendered risks?

There are two main reasons underlying our normative suggestion that the GDPR – and more broadly data protection law – *should* explicitly recognise *gendered* risks. Such a recognition is important for both *symbolic* and *normative* reasons.

a. Symbolic significance: Gendered risks and epistemic (in)justice

[190] Maria Tzanou 'Addressing Big Data and AI Challenges' in M Tzanou (ed), *Health Data Privacy under the GDPR* (Routledge 2021) 106–32.
[191] Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015).
[192] Danielle Keats Citron and DJ Solove, 'Privacy Harms' (2021) 102 *Boston University Law Review* 793.
[193] Kimberle Crenshaw 'Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Colour' (1991) 43 *Stanford Law Review* 1241; Shelby, Imad Harb and Henne (n 115) at 3.

We argue that in light of the 'likelihood', 'severity' and 'possible consequences'[194] of producing systemic harms to women and girls at both the individual and the societal level as identified above, the lack of an explicit recognition of an adverse impact related to gender of personal data concerning them would constitute at a s*ymbolic* level an *epistemic injustice*.

In her ground-breaking work, Miranda Fricker theorised the intersection of social epistemology with theories of justice. Fricker identified two distinctively epistemic forms of injustice: *testimonial injustice*, which 'occurs when prejudice causes a hearer to give a deflated level of credibility to a speaker's word' and *hermeneutical injustice* which 'occurs when a gap in collective interpretive resources puts someone at an unfair disadvantage when it comes to making sense of their social experiences'.[195] While both forms are relevant here, we focus on hermeneutical injustice which directly links with our discussion of the law (here: the GDPR). Hermeneutical injustice is structural because it arises when a society lacks the interpretive resources to make sense of a speaker's experience, because they or members of their social group have been 'prejudicially marginalized in meaning-making activities'.[196] The example used by Fricker to explain hermeneutical injustice is illuminating in the context of the present discussion. As Fricker explained, prior to the introduction of the concept of sexual harassment into public and institutional discourse, people tended to interpret women's experiences and trauma at unwanted sexual advances as 'hysterical reactions to innocent flirtation'.[197] Sexually harassed women suffered *hermeneutical injustice* because they lacked the interpretive resources to make sense of the injustice

[194] This is the language used by the CJEU in recent cases regarding non-material damages under the GDPR. For instance, in NAP the Court held that 'the risks of a personal data breach caused by the processing concerned, more specifically the likelihood and severity thereof, and the possible consequences for the rights and freedoms of natural persons need to be assessed'. See Case C-340/21 *VB v Natsionalna agentsia za prihodite* EU:C:2023:986.
[195] Miranda Fricker, *Epistemic Injustice: Power and the Ethics of Knowing* (OUP 2007) 1.
[196] Fricker (ibid), 158–59; Elizabeth Anderson, 'Epistemic Justice as a Virtue of Social Institutions' (2012) 26 *Social Epistemoly* 163, 166.
[197] ibid.

they were suffering, due to their prejudicial epistemic marginalization: women were expected to put up with what was considered 'normal' male behaviour.[198]

While Fricker's hermeneutical injustice theory focuses primarily on the individual level and proposes epistemic virtue as a solution,[199] it is an important analytical framework through which one can consider gender concerns in the GDPR (or the absence thereof). Unlike Fricker, who focuses on the speaker's experiences (eg, those of harassed women), hermeneutical injustice concerns here the *institutional* (the *legislative*) level and, in particular, *how* epistemic injustice may be constructed through legal frameworks and policies. Feminist theory has long discussed 'the way in which relations of power can constrain women's ability to understand their own experiences'.[200] As Nancy Hartsock noted, 'the dominated live in a world structured by others for their purposes—purposes that at the very least are not our own and that are in various degrees inimical to our development and even existence'.[201] Social institutions and practices are structured 'to favour the powerful' and, from an epistemological point of view, 'the powerful have an unfair advantage in structuring collective social understandings'.[202] This entails that 'in the hermeneutical context of social understanding, … if understandings are structured a certain way, then so are the social facts'.[203]

The explicit recognition of gendered concerns in data protection law is, therefore, significant at a *symbolic* level. This recognition would address the above issue of institutional epistemic injustice and make the GDPR an even more robust fundamental rights' legal instrument which concerns itself with – so far – largely neglected data protection issues. Such a recognition is urgently needed as emerging technologies increase the surveillance capabilities of women's bodies, thereby incurring gendered risks.

---

[198] ibid.
[199] ibid.
[200] Fricker (n 195) at 148.
[201] Nancy Hartsock, *The Feminist Standpoint Revisited and Other Essays* (Westview Press 1998) 241.
[202] Fricker (n 195) at 148.
[203] ibid.

This recognition departs from the current GDPR approach and would, therefore, require legislative intervention. In practice, it could be incorporated in one of the GDPR's numerous recitals or included where it provides examples of 'risk' and 'risky processing'. For instance, the GDPR recognises that children require additional protection, particularly in relation to information society services, because they are considered to be 'vulnerable'.[204] It would certainly be important to also acknowledge the data protection risks that girls face daily with regard to menstruation and, more broadly, their sexual and reproductive rights.

It goes without saying that *de lege ferenda*, it would be even more preferable if gender (as well as sexual and reproductive rights) were explicitly recognised in Article 9 of the GDPR which, unlike its recitals, is legally binding. This would better address the issues of epistemic injustice identified above.

b. Normative significance: Gendered risks and the GDPR's risk-based approach

An explicit recognition of gender (and gendered risks) within the GDPR is also significant due to its *normative* implications. In particular, the weaknesses of the risk-based approach, identified in Part 2, lend support to the need for a recognition of gendered risks.

First, the ambiguity surrounding the meaning of risk has implications for the implementation of the risk-based approach. As discussed above, GDPR-mandated accountability obligations are scalable, meaning that their scope should be calibrated based on the risks posed to natural persons, specifically the likelihood and severity thereof. Neglecting to identify and manage an entire category of risks (here gendered ones) entails that controllers' accountability obligations are inaccurately calibrated. Such omission, and accordingly such inaccurate scaling, is striking when it comes to gendered risks, which can both be highly likely (since they affect users simply by

[204] See, inter alia, Recitals 38 and 75, as well as GDPR, art 8 (n 2).

virtue of their gender) and highly severe (since they can cause bodily, reproductive harms). Therefore, an explicit recognition of gendered risks is necessary for the accurate scaling of controllers' accountability obligations and, more concretely, for the implementation of appropriate technical and organisational measures in service of compliance.

In line with the preceding conceptualisation of gendered risks, as well as the understanding of risk as a scenario describing both an event and its consequences, such a recognition should be broad. It should consider not only gendered processing and the processing of gendered personal data (event) but also the gender-related impacts of such processing (consequences), even when the latter is gender neutral (eg, in cases where compliant data processing may nonetheless lead to technology-facilitated gender-based violence or other violations of bodily integrity). It should, likewise, be broad in terms of the type of risk, including digital as well as embodied, tangible as well as intangible. Beyond the individual-level risks that are currently captured by the GDPR, such a recognition of gendered risks should finally be broad in terms of the risk subjects, encompassing groups/collectives and the society at large, as well as individuals.

Second, as the GDPR does not impose a general, independent obligation to protect natural persons' rights and freedoms (but rather one contingent on the compliance of data processing), the relation between rights and risks, and the scope of rights to be considered, remain unclear. The explicit inclusion of gendered risks into the GDPR's risk-based approach is therefore needed to expand the scope of rights under consideration and include sexual and reproductive health rights. As demonstrated, reproductive rights are necessary to the enjoyment of other fundamental rights yet often threatened by data-driven technologies, including femtech. Following the WP29's guidance on the scalability of risks versus rights, consideration and respect of such reproductive rights should be upheld even when the data processing itself is of low risk.[205]

[205] Article 29 Data Protection Working Party, WP 218 (n 13).

Third, given the ambiguities surrounding its exact meaning and scope, the risk-based approach is largely left to the controllers' interpretation, which may or may not include input from data subjects, despite the fact that risk is often subjective and hard to objectively assess. This exclusive reliance on controllers is problematic if we consider that, following general trends in the IT industry, many developers and owners of, for instance, the for-profit femtech products and services are not of the same gender as the users of said products and services.[206] It is therefore less likely that they will, on their own initiative, identify and anticipate gendered risks, of which they will probably lack first-hand experience. Yet, when these developers and owners act as data controllers, their interpretation of the risk-based approach will, for the most part, be binding. To counter, therefore, controllers' blind spots (in the femtech context and beyond), the possibility of gendered risks should be expressly and authoritatively acknowledged in the law rather than relegated to controllers' self-regulatory initiatives.

(iii) A more moderate re-thinking of the GDPR: Making data protection law gender-responsive *de lege lata*

Above we called for legislative intervention that would incorporate gender in the GDPR—for instance, through one of its recitals or its substantive provisions. However, we acknowledge that such a legislative intervention is not forthcoming, at

[206] For example, popular femtech apps Flo, Glow and Ovia have male CEOs and (co-)founders at the time of writing: C Tucker, '"Our Goal Is to Showcase What Femtech Can Accomplish and That It Is Worth Investing in": Interview with Flo's (the Period Tracker App) CEO and Co-Founder, Dmitry Gurski' (*EU-Startups*, 22 September 2021). Available at: www.eu-startups.com/2021/09/our-goal-is-to-showcase-what-femtech-can-accomplish-and-that-it-is-worth-investing-in-interview-with-flos-the-period-tracker-app-ceo-and-co-founder-dmitry-gurski/; Glow, 'About Glow: Revolutionizing Women's Health Through Data & AI' (*Glow*, 20 May 2023) Available at: www.glowing.com/about-glow; Forbes, 'Paris Wallace | CEO - Ovia Health' (*Forbes Business Council*). Available at: www.councils.forbes.com/profile/Paris-Wallace-CEO-Ovia-Health/68645c4f-8a41-4631-99d8-8f2afd9ee7be#:~:text=Paris%20Wallace%20is%20CEO%20of,women%20and%20families%20since%202012. On the general trends about female representation in IT with a specific focus on the EU context, see: European Parliament, 'European Parliament Resolution of 21 January 2021 on Closing the Digital Gender Gap: Women's Participation in the Digital Economy (2019/2168(INI))' (P9_TA(2021)0026, 21 January 2021).

least in the near future. How could we then re-imagine the GDPR—and the data protection ecosystem more broadly—to meet the need for a recognition of gendered risks? In keeping with existing arguments in the literature, we agree that, beyond the realm of gender, the GDPR should broadly complement its atomistic focus on individual data subjects' protection with an equivalent focus on the collective and societal, systemic risks incurred by data-driven technologies.[207] Such legislative changes would be welcome, but probably hard to achieve, so in what follows we propose at least four other (non-legislative) ways to put gendered (especially collective) risks at the forefront of data protection.

First, contrary to their more common individual rendering, data controllers could perform collective DPIAs; we call these, 'Gender-focused DPIAs' or indeed 'Feminist DPIAs'.[208] The development of such sector-, technology- or target group-specific DPIA frameworks would be better suited to account for the more collective sorts of risks and consequences on particular groups. In particular, a (femtech) sector-specific approach to DPIA frameworks would be able to draw on the accumulated sectoral knowledge and address risks arising from relevant data processing activities in a more targeted, detailed manner. This is recommended by the WP29 itself, which suggests that 'a single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing'.[209] More concretely, this applies to cases of (i) data processing within a particular sector; (ii) use of similar technologies for data processing; or (iii) similar data processing activities.[210] Such collective DPIAs would consider not only high-risk processing but also broader risky outcomes (ie, potential violations of rights, including sexual and reproductive rights).

[207] Inge Graef and Bart van der Sloot, 'Collective Data Harms at the Crossroads of Data Protection and Competition Law: Moving Beyond Individual Empowerment' (2022) 33 E*uropean Business Law Review* 153.
[208] Alessandra Calvi, 'Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection' (2024) 53 *Computer Law & Security Review* 1.
[209] Article 29 Data Protection Working Party, WP 248 (n 25).
[210] ibid.

It is crucial that data subjects' engagement is sought by controllers in developing 'Feminist DPIAs'. Given that risks are varied and often subjective, their assessment would benefit from becoming more participative. Facilitated by Article 35(9) of the GDPR, public involvement could help achieve a more comprehensive framing of the relevant risks, factoring in data subjects' knowledge and context, particularly with respect to gendered risks- be they individual, embodied, collective or societal.

Second, considerations of gendered risks could be made prominent in relevant interpretations and guidance. Recital 77 of the GDPR indicatively suggests the provision of guidance by codes of conduct, certifications, EDPB guidelines and data protection officers, all of which could ensure the inclusion of gendered risks. In that regard, the role of data protection authorities is pivotal. DPAs could specifically direct controllers' attention to gendered risks, raise awareness about these and ensure that data subjects have access to redress mechanisms where such risks materialise. A promising example of such efforts is the recently launched review of period and fertility tracking apps by the UK's Information Commissioner's Office (ICO).[211]

Third, without placing the onus of change on data subjects, their 'strength in numbers' could help address the gendered risks of large-scale data-driven technologies (including femtech).[212] Going back to the discussion of group or collective privacy, data subjects, as groups of citizens and/or civil society organisations, could resort to collective means of defence to address correspondingly collective gendered risks. Such collective action, commonly perceived in law as 'the right to procedural class action and/or to the positive protection of a collective interest' could be taken ex post (eg, through strategic litigation) and ex ante (ie, through preventive measures).[213] Indeed, the provisions of Article 80 of the GDPR leave room for not-for-profit bodies, organisations or associations (e.g., digital rights non-profits, consumer associations,

[211] Information Commissioner's Office (n 153).
[212] Jef Ausloos, Jill Toh and Alexandra Giannopoulou, 'The Case for Collective Action against the Harms of Data-Driven Technologies' (*Ada Lovelace Institute*, 23 November 2022). Available at: www.adalovelaceinstitute.org/blog/collective-action-harms/.
[213] ibid.

trade unions) to start an action on behalf of data subjects (with or without the latter's mandate) albeit under certain conditions and differing national transpositions. Even in the case of (at least seemingly) compliant data processing, data subjects do not necessarily have the (informational or financial) capacity to exercise their rights against resourceful data controllers on an individual basis but may instead require coordination on a collective level.[214] To that end, collectively exercising the right of access has been supported as a means to identify the violation(s) on which subsequent litigation can be based and to help data subjects discern the collective rather than individual risks to which they are exposed. [215]

Fourth, data subjects' engagement could be initiated by local, national and EU policymakers, who would meaningfully include (representatives of) groups that are subject to collective gendered risks across all stages of 'law-making, policy, agenda and strategy setting, litigation, advocacy' as well as 'throughout standardisation processes and broader discussions of technology and digital rights'.[216]

Finally, national and EU courts have an important role to play in recognising gendered risks within data protection law. In particular, the CJEU's widely celebrated pro-data protection/ fundamental rights approach could further develop in this direction to explicitly acknowledge gendered concerns and their link with women's and girls' sexual and reproductive rights.

V. Conclusion

This chapter called for the re-imagination of the GDPR to explicitly recognise gender concerns and argued that its risk-based approach could be a vehicle to achieve this.[217]

---

[214] ibid.

[215] René LP Mahieu and Jef Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards an Ecology of Transparency' (*Internet Policy Review*, 6 July 2020). Available at: www.policyreview.info/articles/news/harnessing-collective-potential-gdpr-access-rights-towards-ecology-transparency/1487; Ausloos, Toh and Giannopoulou (n 212).

[216] Jef Ausloos, Jill Toh and Alexandra Giannopoulou, 'The Role of Collective Action in Ensuring Data Justice' (*Ada Lovelace Institute*, 1 December 2022). Available at: www.adalovelaceinstitute.org/blog/data-collective-action-justice/.

[217] The need to recognise gendered risks could also support an argument for the re-imagination of other, similarly risk-based, legislative instruments. For instance, the EU AI Act explicitly refers to sex and gender, which lends support to the inclusion of relevant considerations in the GDPR, while also

Indeed, risk is central to the GDPR: it is the object and outcome of data protection regulation, as well as a feature of its regulatory approach. However, the current lack of specification about the conceptualisation and measurement of risk, its complex or even antagonistic relation to rights, and the kinds of knowledge or involvement required for its assessment raise several conceptual and practical challenges.

This lack of specification eventually jeopardises data subjects' protection by obscuring the applicability of data subjects' rights and data protection rules more broadly. Focusing on gender, we submitted that while a risk-based approach is central to the GDPR, the possibility of risks or harms of data processing being *gendered* has not, so far, been considered in the law, the case law or the academic literature surrounding EU data protection law. This chapter attempted to fill this regulatory and knowledge gap by conceptualising *'gendered risks'* and by identifying different categories beyond the GDPR's narrow focus on individualistic risks. Despite the conceptual difficulties that the GDPR's risk-based approach poses, we consider that this is the best way to bring gender concerns within its scope, as these cannot be fully and effectively captured by looking merely at potentially gendered personal data, or by considering the (gendered) data subject as 'vulnerable'. In this regard, we argued that a focus on *gendered risks* provides a more dynamic and flexible model, which aligns well with the GDPR's risk-based approach and toolkit on risks mitigation, while probing a reflection on a broader understanding of risks than the one currently envisaged under the GDPR's atomistic focus.

We defined *gendered risks* as risks to the rights and freedoms of natural persons *related to gender* and arising from personal data processing. This conceptualisation of gendered risk focuses on the likelihood of personal data processing resulting in an adverse effect relating to gender; if such a potential adverse effect is likely to materialise this signifies a *gendered risk*. Beyond individual risks, which the GDPR

recognising the possibility of intangible and societal harms. Nonetheless, the concept of vulnerability is again left unclear; the AI Act refers to children and migrants as vulnerable individuals but, other than that, it seems to understand vulnerability as a condition caused by age and physical or mental disabilities.

already recognises, we identified and articulated further types of gendered risks that the GDPR -and more broadly EU data protection law- should be concerning itself with. These include *embodied*, *collective* and *societal* gendered risks. To conceptualise these categories of gendered risks, we focused on femtech as a useful case study at the intersection of data protection and reproductive and sexual rights.

We argued that *embodied* risks, broadly understood as having an impact on bodily integrity, should be recognised because new technologies (such as femtech) increasingly blur the boundaries between data and bodies. Furthermore, the GDPR should acknowledge *collective* gendered risks, which occur when a group experiences a harm in their capacity as a member of that group, and *societal* gendered risks, whose effects might have a systemic and cumulative impact on the lived experiences of women and girls in general.

In light of this, we submitted that the GDPR – and more broadly data protection law – *should* explicitly recognise gendered risks. Such a recognition is important for both symbolic and normative reasons. We acknowledged, however, that this re-imagining of the GDPR to make it gender responsive, would require legislative intervention as it departs from the current 'gender-blind' approach. For the sake of completeness of the discussion, we proposed a number of *de lege lata* ways to put gendered risks at the forefront of data protection law, including feminist DPIAs. Further research – which goes beyond the scope of this chapter – is needed into how feminist DPIAs could be (co-)designed and (co-)implemented in practice so that collective interests are properly considered. We intend to undertake this research in the future, but meanwhile aspire to have opened a new way of thinking about the GDPR's risk-based approach, especially on how this can be developed to incorporate substantive (gender) data justice interests.[218]

[218] Tzanou (n 4); Linnet Taylor 'What is Data Justice?' (2017) 4 *Big Data & Society* 1; Catherine D'Ignazio and Lauren F Klein *Data Feminism* (MIT Press 2020).

Acknowledgment

The research for this paper was funded by the Leverhulme Trust Research Project Grant 'FemTech surveillance: Gendered digital harms and regulatory approaches', RPG-2022-015. The drafting of sections 2, 4.2.2 and 4.3 is primarily attributed to Anastasia Siapka; that of sections 3, 3.2, 4, 4.1, 4.2 and 4.2.1 to Maria Tzanou; and, that of section 3.1 to Anna Nelson. Sections 1 and 5 were co-drafted. The whole manuscript is shaped by all authors and supported by Anna Nelon's research assistance.