THE FUTURE OF EU DATA PRIVACY LAW: TOWARDS A MORE EGALITARIAN DATA PRIVACY

Maria Tzanou*

* Forthcoming in *Journal of International and Comparative Law*, December 2020*

Abstract: The article addresses the future of European Union (EU) data privacy law and argues for a shift of paradigm, calling for a less technology-driven and more human-centric and societally focused approach. It discusses two case studies — poor people's data privacy and women's data privacy — and the recent System for Risk Indication "SyRI" and finds that the mainstream EU data protection narrative has missed out fundamental questions about the *socio-economic*, *gender* and *intersectional exceptions* of EU data protection law. In this regard, the article argues that EU data protection law should be reconstructed to pursue substantive equality goals. It proposes an egalitarian data privacy project guided by methods that bring forward neglected perspectives and narratives. It concludes that only if EU data protection law is attentive to the inequalities that the most vulnerable face, it can remain relevant in the future.

Keywords: *EU data protection law; GDPR, privacy; digital welfare state; benefit fraud; SyRI, women's data privacy; intersectionality; non-discrimination; egalitarian data privacy*

---

*School of Law, Keele University, Staffordshire, ST5 5BG, UK. m.tzanou@keele.ac.uk. Her research focuses on European constitutional and human rights law, privacy, data protection, AI, big data, surveillance and transatlantic data privacy cooperation. She is the author of *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing, 2017) and the editor of *Personal Data Protection and Legal Developments in the European Union* (IGI Global, 2020) and *Health Data Privacy under the GDPR. Big Data Challenges and Regulatory Responses* (Routledge, 2021). The author would like to thank Elaine Fahey and the reviewers for their comments on a previous version of this article.

I. Introduction

Data protection in the European Union (EU) seems to be at its peak. Data protection has been recognised as a fundamental right alongside the right to privacy;[1] it has been modernised to face the information technology-driven challenges of the 21st century through the adoption of the General Data Protection Regulation (GDPR);[2] and, the Court of Justice of the EU (CJEU) has delivered a series of seminal decisions that mark a significant vindication of data privacy vis-à-vis modern electronic surveillance techniques,[3] confirm the extraterritorial application of EU data privacy rights,[4] and show big technology companies (big tech) such as Google and Facebook that they cannot operate in a human-rights free zone in the EU.[5] Primary and secondary data protection law is surrounded by an impressive amount of soft law, reports, guidelines and recommendations by independent authorities and bodies specialising on data protection both at the national (the Data Protection Authorities or DPAs) and at the EU level, the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB). EU data protection law (both hard and soft) is further complemented by an even more impressively rich legal academic scholarship that spans across several hundreds of EU data protection books and textbooks, thousands of journal articles including a journal dedicated to EU data protection law,[6] data privacy studies, blogposts and data protection conferences and workshops.

---

[1] Article 8 of the European Union Charter of Fundamental Right (EUCFR). Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing, 2017).

[2] 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 L 119/1.

[3] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, EU:C:2014:238.

[4] Case C-362/14 *Schrems v Data Protection Commissioner*, EU:C:2015:650.

[5] Case C-131/12 *Google Spain SL*, EU:C:2014:317.

[6] *European Data Protection Law Review* (EDPL).

If data protection law seems to be currently living its best moment, how will the future of EU data protection look? Most would answer this question by looking at the technological challenges data protection is facing. How can data privacy address big data, Artificial Intelligence (AI) and other data-driven technologies? Is data protection law becoming outdated due to rapid technological change?

Not underestimating the importance of technological challenges for the future of data protection, I wish to introduce a novel argument. If EU data protection law wishes to remain relevant in the future, mainstream EU data protection narratives need to be extended to include largely ignored data privacy problems affecting marginalised groups. This article submits that the future priorities of EU data protection law should not be technology driven. Rather than trying to catch up with new technologies, I call for a shift of the current focus of EU data privacy law from technological problems to societal problems of situationally disadvantaged parties that tend to go unremarked. In this respect, this article argues that the future focus of EU data protection law should be in developing an *egalitarian* EU data privacy law.

The analysis proceeds as follows: Section II outlines the contemporary popular narrative of EU data protection law and highlights its limitations. Section III "What the Contemporary EU Data Protection Narrative Has Overlooked", explores the importance of broadening the methodological debates surrounding EU data protection law by discussing two case studies — poor people's and women's data privacy — and addressing questions of intersectionality in the light of the recent System for Risk Indication "SyRI" case. Section IV addresses the future of EU data privacy law and proposes a project of egalitarian EU data protection law. Section V offers brief conclusions.

II. The Contemporary Focus of EU Data Protection Law

The current focus of EU data protection law can be characterised as *technology driven* and *Court centred*.

A. *Technology-driven law*

The emergence and evolution of EU data protection is closely linked to the growing potential of information and communication technology (ICT).[7] The first EU legislative instrument on data protection, the Data Protection Directive (DPD) noted that "progress (…) in information technology" made the processing and exchange of personal data considerably easier.[8] Article 8 of the European Union Charter of Fundamental Rights (EUCFR) elevated data protection to the status of a fundamental right in the EU prompting commentators to applaud the inclusion of a 21st-century technology right in EU's primary law. The current centrepiece EU data protection legislation, the GDPR, is also vocal of its aims to address technological challenges[9] and contains a series of substantive provisions that concern the impact of new technologies on personal data processing. For instance, it imposes an obligation on controllers to undertake a data protection impact assessment (DPIA) "where a type of processing in particular using new technologies, (…) is likely to result in a high risk to the rights and freedoms of natural persons"[10] and attempts "to address the risks arising from profiling and automated decision-making".[11] Finally, the proposed ePrivacy Regulation will replace the ePrivacy Directive[12] as the latter "has not kept pace with technological developments, resulting in a void of protection of communications conveyed through new services".[13]

---

[7] Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) pp.8–9.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 Recital 4 and art.33.

[9] See Recital 6 of the General Data Protection Regulation (GDPR).

[10] Article 35(1) of the GDPR.

[11] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6.

[12] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications) [2002] OJ L 201/37.

[13] Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic

The CJEU has also adopted a technology-driven interpretation of data protection law. In this respect, it often cautions about the capabilities of new technologies and how these touch upon the fundamental rights to privacy and data protection. According to the Court, the effect of the interference with the fundamental rights to privacy and data protection is "heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous".[14] In *Digital Rights Ireland* the CJEU annulled the Data Retention Directive[15] on the basis that this required the retention of all traffic data concerning fixed and mobile telephony and Internet access of all subscribers and registered users. According to the Court such data, taken as a whole, is liable to allow "very precise conclusions to be drawn concerning the private lives" of individuals, such as "everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".[16]

Academic discourse on data protection is also dominated by problems arising in the information age. The ability of data protection law to grasp with questions regarding the Internet, big data, ambient technologies, machine learning and AI features prominently in academic debates.[17]

There is nothing inherently wrong with the technological-driven focus of data privacy law. Data protection rights and interests are particularly pertinent in the information society and data protection laws should provide mechanisms to address technological risks. However, the perpetual quest of data protection law to catch up with new technologies overshadows

---

communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (Brussels, 10 January 2017) COM (2017) 10 final, 2.

[14] *Google Spain SL*, EU:C:2014:317 [80].

[15] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

[16] *Digital Rights Ireland*, EU:C:2014:238 [27].

[17] See Tal Zarsky, "The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making" (2016) 41 *Science, Technology, & Human Values* 118.

other problems that data protection should be concerning itself with. By putting technology and the power imbalances this creates as its main focus, the popular data protection narrative has paid little attention to various data privacy inequalities disproportionally burdening marginalised populations. The obsession to address through EU data protection law the latest technological hype — be that AI or big data — is problematic. As Koops has rightly argued this ends up stretching the concept of personal data "sometimes to the point of breaking, or perhaps rather of becoming void of meaning", or stretching the regulatory problem so that it becomes a problem of processing personal data.[18] I argue that this focus may be motivated by selective interests as well. It seems that data protection is asked to deal predominantly with problems that affect the average and elite individuals.[19] These often concern themselves with the knowledge and power asymmetries that new technologies impose on the many and more privileged in our society. The problem is not merely about stretching the boundaries of EU data protection law and, thus, possibly turning this into "the law of everything"[20] or indeed "the law of nothing"; more crucially, the problem is that this law is becoming troublingly inegalitarian.

B. *CJEU-centred law*

The CJEU's case law has been a driving force for the development of EU data protection law. Indeed, the CJEU has not just had a saying in clarifying the scope of this law, by explaining the meaning of concepts such as "personal" and "sensitive" data, "processing" and "adequacy" of protection for international data transfers; it has consistently interpreted an internal market harmonisation instrument (the DPD) in a manner that fosters the protection of fundamental rights by distancing it from its economic objectives.[21] More recently, the CJEU

[18] Bert-Jaap Koops, "The Trouble with European Data Protection Law" (2014) 4(4) *International Data Privacy Law*, 250, 258.

[19] See Mary Anne Franks, "Democratic Surveillance" (2017) 30 *Harvard Journal of Law and Technology* 425.

[20] Nadezhda Purtova, "The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law" (2018) 10 *Law, Innovation and Technology* 40.

[21] Maria Tzanou, "Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case-Law of the European Court of Justice on Data Protection" (2010) 6 *Croatian Yearbook of European Law and Policy* 53.

sometimes went "beyond the limits of interpretation" and manipulated the texts[22] to create a "super" fundamental right to data privacy[23] that could "effectively make the entire Internet subject to EU data protection law".[24]

Much as the CJEU's data privacy jurisprudence still continues to surprise, what is important for the present analysis is that it sets the agenda and monopolises the mainstream EU data protection debates. Data protection issues considered by the CJEU are the topics that mostly preoccupy EU data privacy scholars. Arguably, these issues are far from unimportant — after all they might concern the EU's digital domination over the whole Internet — but the foregrounding of the CJEU's case law in data privacy scholarship raises questions of what Gestel and Micklitz have called "herd behaviour", namely researchers "choose to follow 'hot topics' and trends",[25] such as these coming before the CJEU.

As in the case of new technologies, this is again dangerously limiting the focus of the EU data privacy debate. EU judges are bound to decide on the particular disputes that reach them using the interpretative methods they commonly apply.[26] Copying these to legal scholarship does not merely complicate "a critical assessment of the output" of the Court;[27] it implies some sort of selection bias that determines what matters are important for EU data protection law and which mainstream ideas and methodologies can be used to approach these. Furthermore, while EU data privacy scholarship is often very critical of the Court and the

---

[22] Oreste Pollicino, "Data Protection and Freedom of Expression beyond EU Borders: EU Judicial Perspectives" in Federico Fabbrini et al (eds) *Data Protection Beyond Borders* (Hart Publishing, 2020 forthcoming).

[23] *Google Spain SL*, EU:C:2014:317, [81].

[24] Maria Tzanou, "European Union Regulation of Transatlantic Data Transfers and Online Surveillance" (2017) *Human Rights Law Review* 545, 553.

[25] Rob Gestel and Hans-Wolfgang Micklitz, "Why Methods Matter in European Legal Scholarship" (2014) 20 *European Law Journal* 292, 305.

[26] Daniela Caruso and Fernanda Nicola, "Legal Scholarship and External Critique in EU Law" in Tamara Perišin and Siniša Rodin (eds), *The Transformation or Reconstitution of Europe: The Critical Legal Studies Perspective on the Role of the Courts in the European Union* (Hart Publishing, 2018) pp. 221, 230.

[27] Gestel and Micklitz, "Why Methods Matter in European Legal Scholarship" (n 25) 299.

consequences — intended or unexpected —[28] of its judgments, the critique that it voices largely focuses on the CJEU's interpretative results and their flaws and misses broader problems that might lead to deficits of substantive justice. Questions on what role EU data protection law can play in eliminating privilege, or class, race and sex inequalities[29] are crucial; yet, these rarely, if ever, reach the CJEU.

III. What the Contemporary EU Data Protection Narrative Has Overlooked

The above analysis has demonstrated that there is a hierarchy in EU data privacy problems: those that concern the latest technological innovation and questions that arise from the CJEU's case-law attract more attention. The problem, however, is that this technologically driven, CJEU-centred focus of EU data protection law has not bothered to concern itself with the fundamental question: Data protection *for whom*? Are only the interests, experiences and problems of the relatively privileged members of society that matter? Are data privacy law outcomes equally distributed? What are the issues that the more vulnerable and disadvantaged face in this respect?

This section takes a closer look at examples of what I argue has been left behind by the mainstream EU data protection law narrative: *poor people's* and *women's* data privacy.

A. Poor people's data privacy

In his Report to the United Nations (UN) General Assembly, the Special Rapporteur on extreme poverty and human rights, Professor Philip Alston details the emergence of the "digital welfare state".[30] Systems of social protection and assistance worldwide,[31] including in

[28] Maria Tzanou, "The Unexpected Consequences of the EU Right to Be Forgotten" in Maria Tzanou (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global, 2020) p.279.

[29] Caruso and Nicola, "Legal Scholarship and External Critique in EU Law" (n 26) p.230.

[30] Report of the Special Rapporteur on extreme poverty and human rights, 11 October 2019, A/74/493.

many EU countries, (commonly known as the "welfare state") that provide a range of government services and goods to underprivileged persons, such as low-income individuals, job-seekers and persons with disabilities are increasingly employing digital technologies to "automate, predict, identify, surveil, detect, target, harass and punish" their beneficiaries, "especially the poorest and most vulnerable among them".[32] Digital innovation is used by the welfare state to verify the identity of benefits applicants (requiring often the retention of biometric data); assess their eligibility; calculate payments benefits; prevent and detect welfare fraud; and, calculate risks. In the Report, the Special Rapporteur laments that:

> unrestricted data-matching is used to expose and punish the slightest irregularities in the record of welfare beneficiaries (while assiduously avoiding such measures in relation to the well-off); evermore refined surveillance options enable around-the-clock monitoring of beneficiaries; conditions are imposed on recipients that undermine individual autonomy and choice in relation to sexual and reproductive choices and choices in relation to food, alcohol, drugs and much else; and highly punitive sanctions are able to be imposed on those who step out of line.[33]

It is hardly new or surprising that the poor are subjected to surveillance. Indeed, the poor have sustained for years pervasive surveillance of their bodies, habits, decisions and homes (or the lack thereof).[34] For instance, the homeless have since long been criminalised for engaging in "activities that would be perfectly legal inside a home: standing or sitting in one place for long periods of time, sleeping, drinking alcohol, and engaging in sexual activity".[35]

What is perhaps more perversely remark worthy about the emergence of the "digital welfare state" is the inherent assumption that the poor are not entitled to data privacy either.

---

[31] On the United States, see Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press, 2018).

[32] Report of the Special Rapporteur (n 30) para.63.

[33] *Ibid.*, para.77.

[34] Robin Morris Collin and Robert William Collin, "Are the Poor Entitled to Privacy?" (1991) 8 *Harvard Blackletter Journal* 181.

[35] Franks, "Democratic Surveillance" (n 19) 444.

The design of the digital welfare system imposes an additional layer of surveillance on poor people, this time a digital one. It requires that they become visible as data points of observation if they wish to be part of this. It is not just that social services beneficiaries are "effectively forced to give up their data privacy rights to receive their right to social security";[36] their condition as being poor and vulnerable denies them any entitlement to data privacy from the outset. Indeed, their condition of being poor implies that the welfare state can single them out; object them to constant monitoring and surveillance; compile and hold databases on them storing personal information they are required to provide; interconnect government data silos and private-sector databases to match this information with further data; score risks on the ways they lead their lives; and even "try to alter social behaviours, such as sexual activity or preferences, approaches to cohabitation, (…) and the decision to have children".[37]

What's more, this is hardly seen as extraordinary; in fact, it is the (new?) normal. As the Special Rapporteur eloquently observes "because of the relative deprivation and powerlessness of many welfare recipients, conditions, demands and forms of intrusiveness are imposed that would never be accepted if they were piloted in programmes applicable to better-off members of the community instead".[38]

The issue of benefit fraud is particularly illuminating in this respect. Benefits claimants are often perceived as "cheats" or "scroungers"[39] and suspected of defrauding the state.[40] Cracking down on benefit fraud is, therefore, considered a legitimate public interest objective. In the United Kingdom, the Cabinet Office conducts every two years the National

[36] Report of the Special Rapporteur (n 30) para.64.

[37] *Ibid.*

[38] *Ibid.*, para.6.

[39] David Garland, *The Welfare State: A Very Short Introduction* (Oxford University Press, 2016).

[40] Brief by the United Nations Special Rapporteur on extreme poverty and human rights as *Amicus Curiae* in the case of *NJCM cs/ De Staat der Nederlanden (SyRI)* before the District Court of The Hague, para.22.

Fraud Initiative (NFI), a massive data matching exercise that amasses data[41] from 1,200 organisations from the public and private sectors including government departments and combines them to identify "potentially fraudulent claims and benefits" in a broad range of areas, including housing benefits, council tax, social housing applications, pension fraud and blue badges.[42]

In the Netherlands, the Dutch government has taken various measures to punish welfare fraud since 2003. For instance, in order to tackle the so-called "living together" benefit fraud (a situation where a claimant declares to be living alone to receive a higher benefit, yet lives with another person), the "Waterproof" (Waterproef) project implemented between 2006 and 2010, matched databases from drinking water companies and public bodies containing information on 63,000 welfare beneficiaries receiving a type of benefit intended for those who have no other forms of income or assets.[43] Water usage was used as a "risk indicator" and the system flagged individuals living at certain addresses as "at risk" for committing "living together" fraud.

The more recent System for Risk Indication "SyRI" (Systeem Risico Indicatie) follows the same trend. It matches personal data[44] from several government silos using a risk calculation model to predict the likelihood of an individual committing benefit or tax fraud or violating labour laws.[45] In a seminal decision delivered in February 2020, the Hague District Court found that SyRI breached art.8 of the European Convention on Human Rights (ECHR) because it failed to strike a right balance between the benefits the use of new technologies

---

[41] Cabinet Office, Statutory Guidance, National Fraud Initiative privacy notice, Updated 17 July 2019, <https://www.gov.uk/government/publications/fair-processing-national-fraud-initiative/fair-processing-level-3-full-text> (visited 31 July 2020).

[42] Cabinet Office, National Fraud Initiative Report, 1 April 2016 to 31 March 2018, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/737146/National-Fraud-Initiative-Report-2018.pdf> (visited 31 July 2020).

[43] Brief by the United Nations Special Rapporteur (n 40) para.13; Valery Gantchev, "Data Protection in the Age of Welfare Conditionality: Respect for Basic Rights or a Race to the Bottom?" (2019) 21 *European Journal of Social Security* 3.

[44] On the data used see Hague District Court, *SyRI*, NL:RBDHA:2020:865, Decision of 5 February 2020, [4.17].

[45] *Ibid.*, [4.23].

bring as regards the prevention and combating fraud on the one hand, and the potential interference with the exercise of the right to respect for private life through such technological use on the other hand.[46]

It is worth taking a closer look at three points of the District court's analysis that are relevant to the present discussion. First, it is worth remarking that while the court decided the case on the basis of art.8(2) of the ECHR, the bulk of its analysis focused on what can be characterised as "data protection problems". In particular, the court considered three data protection principles, the principles of transparency, purpose limitation and data minimisation and, on the basis of these, it found that the legislation pertaining to the application of SyRI was "insufficiently transparent and verifiable".[47] This confirms that data protection law is central for the assessment of systems of risk calculation models. Second, questions about new technologies occupied a large part of the court's analysis. Having noted that the State has a "special responsibility when applying new technologies",[48] the Dutch court embarked, upon the applicants' request, to examine whether SyRI involved a "dragnet, untargeted approach, data mining, 'deep learning', 'big data'; and whether it entailed profiling and automated decision-making".[49] In this regard, the court noted that due to the speed of technological development, "the right to data protection is becoming increasingly important".[50]

While highlighting the importance of data protection in the face of new technologies, the court failed to recognise the discriminatory impact that welfare fraud detection schemes impose on the poorer and more vulnerable in the society. The imposition of an additional layer of surveillance without any cause of suspicion only on a particular segment of the population was not considered as such problematic for the right to data protection. Indeed, it is worth remarking that according to the Hague District court:

> the *starting point* is that social security is one of the pillars of Dutch society and contributes to a considerable extent to prosperity in the Netherlands… The social security system can only function if citizens in the Netherlands who are not eligible

[46] *Ibid.*, [6.6].

[47] *Ibid.*, [6.7].

[48] *Ibid*., [6.84].

[49] *Ibid.*, [6.46]–[6.65].

[50] *Ibid*., [6.85].

> for such facilities do not make use of them. The system is financed with public money and fraud affects the solidarity underlying the system. Combating fraud is therefore key to maintain citizen support for the system.[51]

General citizen support for the welfare system seems, therefore, to be a rationale put forward by the mainstream society (indeed by the State) to tolerate — or even encourage — the surveillance of the poor.[52] Besides being carried out with no previous suspicious of fraud and detecting very few such cases (under the "Waterproof" project 42 benefit frauds were detected overall, amounting to 0.07 per cent), the case of the welfare fraud demonstrates the disparate impact of data privacy. Poor peoples' data privacy clearly *does not matter* enough; this can be denied altogether in the name of detecting benefit fraud. The problem, is not, therefore, that such measures violate several data protection principles and rules, such as purpose limitation, data minimisation, etc.; the problem is that they turn the very concept of data protection on its head. Benefits claimants are not allowed the data privacy the non-claimants enjoy because they might commit fraud. The poorest and more vulnerable in the society are once again seen as "second-class" citizens; this time, with regard to their data privacy rights.

Combatting benefit fraud at the national level is not the only example of the disparate impact of data privacy protections afforded to the vulnerable. At the EU level, the EU operates a "mille-feuille" of databases[53] that are purposefully designed to monitor third-

---

[51] *Ibid.*, [6.3] (emphasis added).

[52] The court noted that while it was correct to date that SyRI had only been applied to so-labelled "problem districts", "this in and of itself need not imply that such use is disproportionate or otherwise contrary to Article 8 paragraph 2 ECHR in all cases". However, it observed that "given the large amounts of data that qualify for processing in SyRI, … and the circumstance that risk profiles are used, there is in fact a risk that SyRI inadvertently creates links based on bias, such as a lower socio-economic status or an immigration background". *Ibid.*, [6.93].

[53] Niovi Vavoula, "The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection" (2020) 45(3) *European Law Review* 348, 349.

country nationals (TCNs) and designate them in "risk groups"[54] in order to sort them out "between bona fide and mala fide and to assign levels of danger".[55] The EU's "smart borders" are used to enable the dehumanisation of migrants on basis of preventative security measures that treat them as suspects per se.[56]

While the Snowden revelations about mass digital surveillance might have created a "chilling effect" in the exercise of the fundamental rights to privacy and freedom of expression of the majority, the harms to the poor and vulnerable from surveillance regimes imposed only onto them go far beyond a "chilling effect". As pointed out by Madden et al, many surveillance systems targeting the poor "are purposefully designed to deliver a message of stigma to the subject while reinforcing societal stereotypes about dependency".[57] Discriminatory and punitive laws, combined with the threat of sanctions, directed at the poor and vulnerable exacerbate long-term health conditions and negatively affect mental health.[58]

To sum up, it seems that data privacy has a differential impact. It is not equitably applicable to everyone; its application depends on personal conditions: the more socio-economically disadvantaged groups are *de facto* expected to have diminished data privacy. Lower levels of data privacy protection are deemed acceptable in contexts of state support and intervention. But these do not apply to "regular" citizens who remain outside these systems. In this respect, data privacy is no longer a right that all can enjoy. It instead turns to a

---

[54] Didier Bigo, "Globalized (In)Security: The Field and the Ban-Opticon" in Didier Bigo and Anastassia Tsoukala (eds), *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11* (Routledge, 2008) 10.

[55] Vavoula, "The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection" (n 53) 366.

[56] Valsamis Mitsilegas, *The Criminalisation of Migration in Europe: Challenges for Human Rights and the Rule of Law* (Springer, 2015).

[57] Mary Madden et al, "Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans" (2017) 95 *Washington University Law Review* 53, 61.

[58] Mandy Cheetham et al, "Impact of Universal Credit in North East England: A Qualitative Study of Claimants and Support Staff" (2019) *British Medical Journal* Open 9:e029611; Sophie Wickham et al, "Effects on Mental Health of a UK Welfare Reform, Universal Credit: A Longitudinal Controlled Study" (2020) *Lancet Public Health* 5:e157.

"privilege" that is distributed depending on who has the means to afford it.[59] This is what I call the *socio-economic exception* of data privacy.

B. Women's data privacy

Women have throughout the history experienced diminished levels of privacy as their bodies have been treated as "property" of their fathers, their husbands, or of men in general.[60] Popular conceptions of privacy have also been criticised by prominent feminists as providing "a shield for domestic violence".[61]

Modern technologies have intensified the surveillance of women. Women must now 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",[62] deepfakes[63] and so on.[64] New forms of surveillance of women's bodies, health and reproductive choices and intimate relations have emerged. Mobile apps and wearable devices have been developed to track periods, provide fertility solutions, manage pregnancy, contribute to sexual well-being and reproductive healthcare and measure sexual

---

[59] Stacy-Ann Elvy, "Paying for Privacy and the Personal Data Economy" (2017) 117 *Columbia Law Review* 1369.

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

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

[62] Franks, "Democratic Surveillance" (n 19) 447.

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

[64] Ian Sample, "Internet 'Is Not Working for Women and Girls', says Berners-Lee", *The Guardian* (12 March 2020) <https://www.theguardian.com/global/2020/mar/12/internet-not-working-women-girls-tim-berners-lee> (visited 31 July 2020); Report of the Special Rapporteur on the right to privacy, 27 February 2019, A/HRC/40/63 para.78.

activity and performance. This range of products, services and software often referred to as FemTech is considered to deliver important benefits for women, including empowering them to assume a more active role in personalised health management and improving overall quality of life. While the promise of FemTech 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 . . .[65]

Women, their bodies, cycles, communications, relationships and activities are constructed as "monitored subjects"[66] that can be seduced, coerced, disciplined and controlled.[67] 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, etc.) to intimate partners and ultimately governments.

Recent examples of women's intimate surveillance by the market are abundant: From the period and ovulation app that was sharing women's period dates with Facebook; and, the use of family-planning apps by employers and health-insurers to control women's fertility and reproductive choices; to revelations that a fertility app with which women share sex and menstruation information was funded by US anti-abortion campaigners, we get a disturbing glimpse into the complexities of information and power asymmetries of the "surveillance capitalism"[68] society.

A disturbing number of "spy" apps exist with the purpose of surreptitiously gathering data about an intimate partner, including reading texts, monitoring social media activity, checking contacts, following GPS locations, downloading media files, and even accessing

---

[65] Deborah Lupton, "Quantified Sex: A Critical Analysis of Sexual and Reproductive Self-Tracking Using Apps" (2014) 17 *Culture, Health & Sexuality* 440.

[66] Karen Levy, "Intimate Surveillance" (2015) 51 *Idaho Law Review* 679, 688.

[67] Rob Kitchin, "Thinking Critically about and Researching Algorithms" (2017) 20(1) *Information, Communication & Society* 14, 19.

[68] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization" (2015) 30 *Journal of Information Technology* 75.

deleted messages.[69] Intimate partner surveillance (IPS) that can also be perpetrated through general social media can cause both emotional and physical harm.[70] In the most extreme cases it can lead to violence, physical assault and even murder.[71] IPS and domestic violence disproportionately affect women. According to a European Parliament report, one woman in three has experienced some form of physical and/or sexual violence and there are approximately 3,500 domestic violence-related deaths in the EU every year. This means that there are more than nine victims, as many as seven of them women every day and over half of all female murder victims are killed by an intimate partner, relative or family member.[72]

Reporting abuse or rape often places women under a further layer of surveillance — this time perpetrated by the State. In the United Kingdom, women reporting rape or other serious sexual offences are required by the police to hand over their mobile phones to allow detectives to search and download call data, messages, email, contacts, apps and Internet browsing history.[73] The phones of victims can be kept by the police "for several months".[74]

---

[69] Lucy Bennett, "10 Free Cheating Spouse App for Android" *iLounge* (3 February 2020) <https://www.ilounge.com/articles/10-free-cheating-spouse-app-for-android> (visited 31 July 2020).

[70] Molly Dragiewicz et al, "Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms" (2018) 18(4) *Feminist Media Studies* 609.

[71] Rahul Chatterjee et al, "The Spyware Used in Intimate Partner Violence" (2018) IEEE Symposium on Security and Privacy, 441 <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418618> (visited 31 July 2020).

[72] Rosamund Shreeves and Martina Prpic, Briefing, Violence against Women in the EU: State of Play, PE 644.190, November 2019.

[73] NPCC, Digital Device Extraction, 29 April 2019 <https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf> (visited 31 July 2020).

[74] NPCC and CPS evidence to the Justice Committee Inquiry into Disclosure in Criminal Cases <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-ofevidence-in-criminal-cases/written/80671.pdf> (visited 31 July 2020).

According to the victims' commissioner for London, such "digital strip searches"[75] of sexual assault victims might be used to create "character assassinations" of victims and cast doubt on their credibility ("victim blaming"), thus, leading to a "high level of victim withdrawals from cases and also the increase in police "no further action" and the decline in …charging decisions".[76] Furthermore, as the National Police Chiefs' Council (NPCC) and the Crown Prosecution Service (CPS) have recognised "denied access to a telephone could cause serious financial and social hardship or risk to personal safety".[77]

In short, data privacy is also gendered. Women are expected to face new forms of digital scrutiny of their bodies, communications, intimate details and habits. They are once again judged, disciplined, controlled and subordinated as it is assumed by default that they enjoy lower levels of data privacy. This is what I call the *gender exception* of data privacy.

C. Intersectionality concerns and data privacy

Writing about black women, Kimberle Crenshaw coined the term intersectionality to describe how some individuals are "multiply-burdened" and experience "combined effects" of discrimination.[78] Intersectionality examines how different categories of inequalities, such as race, gender, class, ethnicity, disability, sexual orientation and age intersect with each other.

---

[75] Big Brother Watch, "Digital Strip Searches: The Police's Data Investigation of Victims", July 2019.

[76] Owen Bowcott and Caelainn Barr, "Impact on Rape Victims of Police Phone Seizures to be Reviewed" *The Guardian* (16 February 2020) <https://www.theguardian.com/society/2020/feb/16/impact-on-victims-of-police-phone-seizures-to-be-reviewed> (visited 31 July 2020). The NPCC has indicated that this practice would be withdrawn by August 2020. Alexandra Topping, "Police and CPS Scrap Digital Data Extraction Forms for Rape Cases" *The Guardian* (16 July 2020) <https://www.theguardian.com/society/2020/jul/16/police-and-cps-scrap-digital-data-extraction-forms-for-cases> (visited 31 July 2020).

[77] NPCC and CPS evidence (n 74).

[78] Kimberle Crenshaw, "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics" (1989) 1 (8) *University of Chicago Legal Forum* 139, 139, 140, 149.

Accounting for intersectionality in the context of the present discussion requires close attention to be paid to the complex and compounding harms of different forms of surveillance on disadvantaged individuals and the impact on their data privacy.

To take another example from the United Kingdom, in response to the 2011 London riots, the Metropolitan Police created a so-called "gangs matrix" that compiled a list of individuals, giving them a "violence ranking" from green, to amber and red. The matrix contained a disproportionate number of poor, young black people (78 per cent)[79] when as the Amnesty International observes in reality black people are responsible for just 27 per cent of serious youth crime.[80] Many of the individuals included in the matrix posed "zero risk" of causing harm, while some were assessed as being much more likely to be victims than offenders.[81] Yet, their personal data stored on the gangs matrix were shared with other public authorities with the concomitant repercussions (some had their driving licences withdrawn or applications denied).[82] The gangs matrix problem demonstrates why intersectionality matters when considering data protection: race, gender, age, ethnicity and socio-economic status may impose multiple layers of surveillance on certain individuals.

IV. An Egalitarian EU Data Privacy Project

Addressing the issues identified above requires dealing with large, systemic and deeply rooted social ills such as poverty, discrimination, gendered, racial and socio-economic subjugation and their multiple and complex underlying causes. These overarching problems can only be

[79] Amnesty International UK, "Trapped in the Gangs Matrix" *Amnesty International* (23 November 2018) <https://www.amnesty.org.uk/trapped-gangs-matrix?gclid=Cj0KCQjwu6fzBRC6ARIsAJUwa2T7qWMA3YtDl1u3ERH4PG-4sII8m393yg4zEzHr7rDxdfZFFeY-RDoaAtKeEALw_wcB> (visited 31 July 2020).

[80] *Ibid.*

[81] Vikram Dodd, "Met Removes Hundreds from Gangs Matrix after Breaking Data Laws" *The Guardian* (15 February 2020) <https://www.theguardian.com/uk-news/2020/feb/15/met-removes-hundreds-from-gangs-matrix-after-breaking-data-laws> (visited 31 July 2020).

[82] *Ibid.*

addressed by an eradication of the substantive conditions of subordination.[83] This article engages in a more modest task: it proposes a project of *de-* and *re-* construction of EU data protection law with the aim of making this more *egalitarian*. This egalitarian reconceptualisation entails a twofold task: (i) to expose the problems of the unarticulated and often invisible inequalities of EU data privacy law and recognise the harms these produce (the *de-construction* of EU data privacy law) and (ii) to integrate these problems into current and future EU data protection discussions and search for tools to address them by advancing substantive equality (the egalitarian *re-construction* of EU data privacy law).

A. Data privacy law matters

It should be stated from the outset that the task of *de*-constructing EU data privacy is not one of negating or discarding the normative and symbolic significance of this area of law or of the relevant fundamental right recognised in art.8 of the EUCFR. It is rather an attempt to re-configure this to advance substantive equality goals. Indeed, my intention is to suggest future improvements for EU data privacy and therefore the starting point of the analysis is to defend *why* this fundamental right *matters*.

It has been argued — by American scholars — that data privacy "dominates the way most judges and scholars think",[84] and such approach is problematic because it "focuses too heavily on information streams…push[ing] arguably higher-stakes privacy invasions to the margins and privileges data over bodies", therefore, obscuring other embodied privacy harms and "other, arguably more significant, privacy interests".[85] With the necessary caveats that EU privacy law differs from US privacy law and these views describe the US framework where privacy protections are sectoral and mainly found in the Fourth Amendment[86] and there

[83] Kimberlé Crenshaw, "Race, Reform, and Retrenchment: Transformation and Legitimation in Antidiscrimination Law" (1988) 101 *Harvard Law Review* 1331, 1341.

[84] David Sklansky, "Too Much Information: How Not to Think About Privacy and the Fourth Amendment" (2014) 102 *California Law Review* 1069, 1103.

[85] Franks, "Democratic Surveillance" (n 19) 452.

[86] Maria Tzanou, "The War against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security?" (2015) 31(80) *Utrecht Journal of International and European Law* 87.

is no recognition of separate rights to privacy and data protection,[87] I submit that establishing hierarchies "of significance" in privacy law is not helpful. Indeed, data privacy is equally important as other forms of embodied privacy. Data protection aims to protect from a range of information-related harms to the human personality and fosters foundational values such as autonomy and human dignity[88] which requires that individuals should not be treated as a means to an end in their digital lives.[89]

Besides the fact that it is becoming increasingly difficult to distinguish "bodies" from their "data doubles"[90] in the information society, the above case studies illustrate that data privacy protections and concerns are crucial for disadvantaged groups. Indeed, the surveillance imposed on the unprivileged is "overt" (rather than the covert surveillance affecting the whole population), and the harms — psychological, material, and physical — suffered by marginalised groups are "concrete" (rather than producing a "chilling effect").[91] Moreover, "an injury sustained by a disempowered group will lack a name, a history and in general a linguistic reality".[92] Fundamental rights matter to the less privileged because they signify "the due, the respectful behaviour, the collective responsibility properly owed by a

[87] Robert Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere" (2018) *Duke Law Journal* 982. Post argues that art.7 of the EUCFR recognises "dignitary privacy" while art.8 recognises a "bureaucratic" and "asocial" "data privacy". I do not think this distinction is accurate. See Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (n 1).

[88] Article 1 of the EUCFR.

[89] Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (n 1).

[90] Kevin Haggerty and Richard Ericson, "The Surveillant Assemblage" (2000) 51(4) *The British Journal of Sociology* 605.

[91] Michele Gilman, "The Class Differential in Privacy Law" (2012) 77 *Brooklyn Law Review* 1389, 1397.

[92] Robin West, "The Difference in Women's Hedonic Lives: A Phenomenological Critique of Feminist Legal Theory" (1987) 3 *Wisconsin Women's Law Journal* 81, 85.

society to one of its own".[93] It is the role of the right to data protection to translate into legal reality the surveillance injuries the more disempowered sustain and offer substantive and procedural methods to remedy these. The current problem with data privacy is that it is not *equitably distributed* to these groups; and *not* that it is less significant for vulnerable communities compared to the more privileged ones.

B. EU data privacy law should be egalitarian

The project of reconstructing EU data privacy law entails a core normative argument. EU data privacy law *should* be egalitarian: it *should* be equally distributed to and equally enjoyed by all persons. This is necessary for both *individual* and *societal* reasons. From the perspective of the individuals affected, an unequal data privacy denies them full respect as citizens[94] and affects their "capacity to live a dignified life".[95] From a societal perspective, such inequalities can perpetuate the subordination of whole groups that lack power in society.[96] Distinctions

---

[93] Patricia Williams, "Alchemical Notes: Reconstructing Ideals from Deconstructed Rights" (1987) 22 *Harvard Civil Rights-Civil Liberties Law Review* 401, 416. See also Privacy International, "From Oppression to Liberation: Reclaiming the Right to Privacy", November 2018.

[94] Gilman, "The Class Differential in Privacy Law" (n 91) 56.

[95] European Union Agency for Fundamental Rights (FRA), "Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement" (2019) 20 <fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf> (visited 31 July 2020).

[96] Judy Walsh, "Unfamiliar Inequalities" (2006) 57 *Northern Ireland Legal Quarterly* 156, 180; Ruth Colker, "Anti-Subordination Above All: Sex, Race, and Equal Protection" (1986) 61 *New York University Law Review* 1003; Elizabeth Coombs, "Gender issues arising in the digital era and their impacts on women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics" — A Report of Consultation by the SRP Thematic Taskforce 'Privacy and Personality'; Report of the Special Rapporteur (n 64), Annex 2, para.99.

between "us" and "them" can reinforce prejudices[97] against the more vulnerable. The serious curtailments of data protection of disadvantaged groups may ultimately influence "the functioning of democracy, since privacy is a core value inherent to a liberal democratic and pluralist society" and affect the trust of the less privileged in public institutions and corporations.[98]

This normative requirement does not extend the scope of EU data protection law. Non-discrimination[99] has been a core value that data protection laws aim to safeguard,[100] and scholars have since long commented on the convergence of anti-discrimination and data protection law.[101] The GDPR states that fair processing requires the prevention of "discriminatory effects"[102] and acknowledges that there are risks to the rights and freedoms of persons which "could lead to physical, material or non-material damage" where "the processing may give rise to discrimination".[103]

Despite these synergies between data protection and anti-discrimination law, however, I argue that an egalitarian understanding of data protection is needed as there are several problems that, even, an "integrated vision of anti-discrimination and data protection law"

---

[97] Opinion of AG Poiares Maduro in Case C-524/06 *Huber v Bundesrepublik Deutschland* EU:C:2008:194, [15].

[98] FRA, "Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement" (n 95) 4 and 28.

[99] Article 21 of the EUCFR.

[100] Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (n 1) 28. See also arts.9 and 10 of the GDPR and Case C-524/06 *Huber v Bundesrepublik Deutschland*, EU:C:2008:724.

[101] Raphaël Gellert et al, "A Comparative Analysis of Anti-discrimination and Data Protection Legislations" in Bart Custers et al (eds), *Discrimination and Privacy in the Information Society* (Springer, 2013) p.81; Philipp Hacker, "Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law" (2018) 55 *Common Market Law Review* 1143, 1171.

[102] Recital 71 of the GDPR.

[103] Recital 75 of the GDPR.

cannot resolve.[104] This is, first, because the scope of EU anti-discrimination law is limited both *ratione materiae* and *ratione personae*: only certain persons in the context of certain relations[105] are protected on the basis of certain grounds. For instance, socio-economic status is not a "protected characteristic" under EU anti-discrimination law.[106] This means that the issues concerning the poor and socially disadvantaged identified above are outside its purview. Second, the centre of gravity of the problems discussed in the case studies concerns data privacy rather than anti-discrimination law. To put it differently, they are often about the disparate impact of surveillance and concomitantly of data protection rather than discrimination *per se*. Data privacy is, therefore, the appropriate forum in principle to discuss these problems.

A first major implication of the normative assumption of the egalitarian project is that data protection should not be used as a legitimising tool for discriminatory kinds of processing. In *SyRI*, the Dutch court assessed the compatibility of benefit fraud detection schemes on the basis of certain data protection principles and rules (data minimisation, purpose limitation, etc). This means that data protection was understood in this context as a permissive tool that enables the exercise of power on the basis of certain principles. Indeed, data protection appears to legitimise the adoption of such schemes, as soon as these comply with some basic fair information principles even if they target the most vulnerable.

Such interpretations cannot be accepted under an egalitarian theory. Data protection law should be able to both regulate and prohibit power.[107] The problem is not how to construct such discriminatory schemes in order to comply with data protection principles; the

---

[104] Hacker, "Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law" (n 101) 1179.

[105] In matters of employment and occupation and with regard to access to (and supply of) goods and services which are available to the public.

[106] See Orla Lynskey, "The Power of Providence. The Role of Platforms in Leveraging the Legibility of Users to Accentuate Inequality" in Martin Moore and Damian Tambini (eds), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press, 2018) p.176. It should be noted that "protected characteristics" under discrimination law and the grounds mentioned in art.9 of the GDPR do not coincide.

[107] Maria Tzanou, "Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not So New Right" (2013) *International Data Privacy Law* 88, 99.

problem is that these are based on discriminatory assumptions and should be, therefore, prohibited as such. Data protection should no longer function only as an enabling tool for measures that violate its "essence".[108] It will merely set out "bureaucratic rules"[109] with no real bite if it cannot call out and prohibit such measures for what they really are: discriminatory, unfairly targeting the most disadvantaged. A reconstructed egalitarian data protection should no longer provide the tools permitting such systems to be built on the basis of the fair information principles; it should be capable to recognise from the outset their disparate impact and — when they violate its essence — prohibit them.[110]

C. Methods matter for an egalitarian data privacy

An egalitarian data privacy project must pay adequate attention to the *socio-economic*, *gender* and *intersectional exceptions* of data protection in order to incorporate these in mainstream debates. This entails a task of "rethinking" data protection law "in relation to the socio-economic, cultural [and] political, … crises that mark our time" and engaging in the ongoing "conversation about the relationship between law and society".[111] I submit that

---

[108] Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (n 1) p.44.

[109] Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere" (n 87) 1011.

[110] Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (n 1). Similar arguments have been made regarding a possible moratorium of Facial Recognition Technologies (FRT). See, Robin Allen and Dee Masters, "Regulating for an Equal AI: A New Role for Equality Bodies — Meeting the New Challenges to Equality and Non-discrimination from Increased Digitisation and the Use of Artificial Intelligence" *Equinet Europe* (Brussels 2020) 43 <https://equineteurope.org/wp-content/uploads/2020/06/ai_report_digital.pdf> (visited 31 July 2020).

[111] Peer Zumbansen, "Transnational Law as Socio-Legal Theory and Critique: Prospects for Law and Society in a Divided World" (2019) 67 *Buffalo Law Review* 909, 928, 931 and 932; Thérèse Murphy, "Human Rights in Technological Times" in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, 2017) 953.

methodological issues matter in this regard because "methods shape one's view of the possibilities for legal practice and reform".[112] Method "organises the apprehension of truth; it determines what counts as evidence and defines what is taken as verification".[113]

An egalitarian data privacy project needs to be oriented by context-sensitive methods that question the operation of EU data protection law and emphasise its "distributive stakes"[114] and consequences. First, EU data protection should be re-positioned in its sociocultural and historical contexts.[115] The lessons from history are fundamental for EU data protection law: the extensive and detailed repositories of personal data stored in government files (census data) and commercial databases (telephone and bank records) in Germany and the Netherlands allowed the Nazis to track down Jews and other "undesirables".[116]

Second, and perhaps more importantly, EU data privacy law should broaden its methodological perspectives by engaging and adapting the analytical, conceptual and empirical toolkits of research agendas and methods such as the "law and society" movement (LSM), Critical Legal Studies, Critical Race Theory and post-colonial legal studies.[117] It is crucial to interrogate EU data protection law through different lenses: gender,[118] intersectional feminist perspectives,[119] critical race studies,[120] critical disability studies,[121] queer studies[122] in

---

[112] Katharine Bartlett, "Feminist Legal Methods" (1990) 103 *Harvard Law Review* 829, 830.

[113] Catharine MacKinnon, "Feminism, Marxism, Method, and the State: An Agenda for Theory" (1982) 7(3) *Signs* 515, 527.

[114] Caruso and Nicola, "Legal Scholarship and External Critique in EU Law" (n 26) p.232.

[115] Reza Banakar, "Having One's Cake and Eating It: The Paradox of Contextualisation in Socio-Legal Research" (2011) 7 *International Journal of Law in Context* 487, 501.

[116] Nicola Jentzsch, *The Economics and Regulation of Financial Privacy: An International Comparison of Credit Reporting Systems* (Springer, 2006) p.140.

[117] See Zumbansen, "Transnational Law as Socio-Legal Theory and Critique: Prospects for Law and Society in a Divided World" (n 111) 912.

[118] Judith Butler, *Gender Trouble: Feminism and the Subversion of Identity* (Routledge, 1990).

[119] Bartlett, "Feminist Legal Methods" (n 112).

[120] Crenshaw, "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics" (n 78).

order to "critically revisit … epistemologies which underlie the conceptual frameworks now in circulation".[123] The employment of these methods can reveal "blind spots" in data protection laws that "fail to account for the inherent power asymmetries and structural disempowerment" of disadvantaged groups.[124] For example, Germany and France do not, for historical reasons, collect any demographic data on ethnicity.[125] However, such data might be necessary to tackle the racial and ethnic injustices deeply ingrained in our "colour-blind" societies.[126] Data protection law cannot be used to justify the "data marginalisation"[127] of groups affected by intersectional discrimination; it should provide the tools to safeguard their rights.

Methods matter not only to identify the problematic distributive consequences of EU data protection law, but also to provide a more explicit recognition of the — often neglected — interests at stake when adjudicating relevant cases. As seen above, in *SyRI* the *starting point* of the court's analysis was that social security is one of the pillars of the Dutch society and therefore benefit fraud must be combatted. Similarly, women that report rape in the United Kingdom must endure a humiliating "digital strip search" because "there is a widespread belief … encouraged by media headlines, that there are a vast number of false

---

[121] Rosemarie Garland-Thomson, "Misfits: A Feminist Materialist Disability Concept" (2011) 26(3) *Hypatia* 591.

[122] Sara Ahmed, "Orientations: Towards a Queer Phenomenology' (2006) 12 *GLQ: A Journal of Lesbian and Gay Studies* 543.

[123] Zumbansen, "Transnational Law as Socio-Legal Theory and Critique: Prospects for Law and Society in a Divided World" (n 111) 916.

[124] *Ibid.*, 920.

[125] Philip Oltermann and Jon Henley, "France and Germany urged to rethink reluctance to gather ethnicity data" *The Guardian* (16 June 2020) <https://www.theguardian.com/world/2020/jun/16/france-and-germany-urged-to-rethink-reluctance-to-gather-ethnicity-data> (visited 31 July 2020).

[126] See the recent Afrozensus initiative in Germany: <https://afrozensus.de/?lang=en> (visited 31 July 2020).

[127] Michele Gilman and Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization" (2018) 42 *New York University Review of Law & Social Change* 253.

allegations of sexual violence".[128] Both these assessments include the inherent assumption that diminished levels of data privacy are acceptable for disadvantaged groups on the grounds that these can be treated as suspects by default and, therefore, other interests are deemed more important than their data protection rights. Public policy objectives are considered in these cases the *starting point* of the analysis instead of the fundamental rights of the vulnerable groups affected. This clearly departs from art.52(1) of the EUCFR and established case law[129] according to which the starting point of the discussion should be the individual's data privacy rights. A more forthright analysis making use of appropriate methods can give a fuller picture of the issues at stake, reject double standards and bring these cases in line with judgments concerning mass surveillance where the starting point of the analysis has been the primacy of data privacy rights.

Finally, methods can direct "the construction of new meanings"[130] and understandings in EU data protection law that will guide appropriately the egalitarian project. For instance, data protection is based on the widely applauded concept of informational self-determination.[131] What are the consequences of this individualistic nature of data protection for vulnerable populations "who experience the intersection of multiple forms of subordination" and the combination of "high-tech", "low-tech", "virtual and physical surveillance"?[132] Should they be expected to also navigate the complexity of data privacy law rules within the context of "corporate and government entanglements"[133] regarding the collection and analysis of their personal information?

---

[128] Big Brother Watch "Digital Strip Searches: The Police's Data Investigation of Victims" (n 75) p.17.

[129] *Digital Rights Ireland*, EU:C:2014:238, [52]; *Schrems v Data Protection Commissioner*, EU:C:2015:650 [92]; Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II)*, EU:C:2020:559 [164].

[130] Bartlett, "Feminist Legal Methods" (n 112) 53.

[131] Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (n 1).

[132] Franks, "Democratic Surveillance" (n 19) 464.

[133] Andrew Selbst and Solon Barocas (eds), AI Now 2017 Report <https://ainowinstitute.org/AI_Now_2017_Report.pdf> (visited 31 July 2020).

V. Conclusion

EU data protection law has over the years seen several celebrated successes as well as setbacks. Both, however, are predominantly centred around the CJEU's case law and the eternal quest of data privacy to catch up with new technologies. This focus of EU data protection law has missed out fundamental questions about the *socio-economic*, *gender* and *intersectional* exceptions of this law.

The most vulnerable and disadvantaged groups are subjected to intensive monitoring and additional forms of surveillance and data protection has often been used as a permissive tool to allow this. This article argued that considering "What's Next?" for the future of EU data protection should encompass questions such as "For Whom"? It called for a shift of paradigm in EU data protection law that should be more human-centric and societally focused.

If we are to seriously consider the future of EU data protection law, this should be reconstructed to pursue substantive equality goals. The egalitarian data protection project proposes a new normative orientation for data protection guided by methods that bring forward neglected perspectives and narratives and ensure its inclusivity and diversity. Only if EU data protection law is attentive to the inequalities that the most vulnerable face, it can remain relevant in the future. It is up to EU data privacy scholars to take the lead in this direction.