Original Research Article

BIG DATA & SOCIETY

Big Data & Society
October–December: 1–13

DOI: 10.1177/20539517241291815
journals.sagepub.com/home/bds
Sage

Digitalisation, democracy and the GDPR: The efforts of DPAs to defend democratic principles despite the limitations of the GDPR

Michaela Padden[1] and **Andreas Öjehag-Pettersson**[1]

Abstract

This article discusses the perspectives of European Union (EU) / European Economic Area Data Protection Authorities (DPAs) on their role in protecting democratic rights and freedoms in digitalised societies. Data Protection Authorities, which are independent regulators, are responsible for implementing the EU's General Data Protection Regulation in their respective countries. The views of DPAs are important given their special role in monitoring newly emerging digital technologies and how their use may impact on the functioning of democracies. The article highlights three key themes which emerged in interviews with 18 DPAs in answer to the question about what they consider to be the greatest challenges to democratic freedoms. These are: (1) threats to elections due to the manipulation of voters; (2) discriminatory effects of automated decision-making; and (3) broader chilling effects on democratic norms due to ubiquitous surveillance. The article then analyses the solutions named by DPAs to mitigate these challenges to identify their governing, or political, rationalities. The paper finds that the solutions available to DPAs to manage democratic harms tend to emphasise individual over collective responsibility and are connected to broader currents of neoliberal governance. The paper highlights the ways in which some DPAs act as important critical voices within their respective jurisdictions to draw political attention to potentially anti-democratic effects of certain practices, such as profiling, or to the model of digitalisation as it is currently constructed.

Keywords

Data Protection Authorities, GDPR, micro-targeting, automated decision-making, chilling effects, profiling

Introduction: Digitalisation and democracy

The principal concern which has given rise to this article is the proliferation, in democratic states, of digital techniques for the purpose of profiling and manipulating people in ways that undermine citizens' democratic rights and freedoms. Specifically, we are interested in the tension between policies which enable these practices on the one hand and efforts to regulate their anti-democratic effects on the other. The European Union's (EU's) General Data Protection Regulation (GDPR) (European Union 2016) is one of several EU Regulations supporting digitalisation across the EU by promoting the 'free flow' (Recital 3; Article 51) of data whilst at the same time minimising risks to democratic rights such as data protection and privacy. Other regulations supporting EU policies to make Europe 'fit for a digital age' (European Commission 2020: 3) include the Artificial Intelligence Act (AI Act) (European Union 2021), the Digital Markets Act (2022a) and the Digital Services Act (European Union 2022b). The purpose of the GDPR, which came into force in May 2018, is to ensure data flows to support the economy and at the same time enforce 'the right to personal data protection' in a manner that is 'balanced against other fundamental rights, in accordance with the principle of proportionality' (GDPR, Recital 4). As such, the GDPR has been considered 'a bulwark for digital democracy' (EDPS 2015).

[1]Faculty of Arts and Social Sciences, Karlstad University, Karlstad, Sweden

Corresponding author:
Michaela Padden, Faculty of Arts and Social Sciences, Karlstad University, Universitetsgatan 2, Karlstad 651 88, Sweden.
Email: michaela.padden@kau.se

Data Protection Agencies (DPAs) in each EU / European Economic Area (EEA) Member State are responsible for enforcing the GDPR. Monitoring and evaluating new technological developments has long been considered a role of DPAs (Simitis 1983; Flaherty 1989), along with functioning as 'an alarm system for the protection of privacy' through reliance on their stock of tools including 'oversight, auditing, monitoring, evaluation, expert knowledge, mediation, dispute resolution and the balancing of competing interests' (Flaherty et al. 1997: 175). They also advise their respective governments on legislative proposals with implications for data protection and privacy. Data Protection Authorities are thus well suited to comment on the challenges posed by digitalisation to democracy given the technological proficiency required of them in their compliance and advocacy work and role as 'guardians of our personal data and our privacy, and of the wider societal interest in privacy as a public good' (Raab and SzeKely 2017: 429, 422).

Surveillance practices are embedded in our current model of digitalisation. Historically, indiscriminate surveillance practices (as opposed to targeted surveillance by law enforcement) and computer-mediated profiling have been considered to have profoundly anti-democratic effects (Lasswell 1971: 195; OECD 1971: 18). Profiling, which lies at the heart of practices of categorising, scoring and deciding, has previously been the subject of research concerning the perspectives of DPAs. It was against this background that the European Commission funded the *PROFILING* project (2012–2014), which surveyed DPAs to identify related risks, awareness and counter-measures in Member States (UNICRI 2013). According to the report's findings, profiling technologies 'clash' with democracy by threatening 'the right to privacy, data protection and non-discrimination, and core values of European societies – democracy, the rule of law, autonomy and self-determination' (Bosco et al. 2015).

Yet in the wake of the 2008 financial crisis, the European Commission promoted data as the 'new gold' and encouraged both the public and private sector to 'start mining it' (European Commission, 2011). Significantly, it did so in the absence of any clear legal framework: '[D]on't wait for this package to become law. You can give away your data now – and generate revenue and jobs [and] new services' (2011). By encouraging a 'Wild West' approach to data appropriation and exploitation, the Commission contributed to what Giraudo (2022: 594) describes as a situation where companies have placed 'bets' on the data they have appropriated and commodified in legally unstable digital markets with 'an over-reliance on the goodwill of private actors as well as on the enforcement priorities of Member States' DPAs' (Giraudo et al. 2024: 4).

Indeed, rapid advancement in computing and information technology has prompted a worldwide race for the best possible position to harness the economic and governmental capacities that are linked to (big) data, algorithms and artificial intelligence (AI) (Cave and ÓhÉigeartaigh 2018). In this sense, data and AI technologies have been identified as strategic resources in the ongoing competition among firms as well as countries, and this new development is often understood to entail significant changes in terms of 'the global distribution of economic, military and political power' (Fischer and Wenger, 2021: 172). Importantly, scholars have also pointed out how this race is not only a race for the resources themselves, but a race of regulation and policy, particularly among the U.S., China, Japan, Canada and the EU (Smuha, 2023). At stake in this race are the values and norms which will underpin the regulatory model or models to eventually dominate AI development and use internationally. How to balance risks and potential benefits in such regulation is an urgent question, not least since the *race* discourse and the quest for competitiveness often follow a rationality where social and political issues are deprioritised in favour of economic potential (Ulnicane, 2023).

Data Protection Authorities are an important link in shaping the values and norms which underpin emerging models of digitalisation. The two core functions of DPAs are shaping and applying data protection law on the one hand, whilst acting as advocates, ombudspersons and administrative authorities on the other (Jóri 2015). According to Jóri, some authorities take an 'activist stance, resembling that of a civil rights advocate', whereas others act more like 'traditional administrative authorities, sticking to narrow (and in some cases rigid) interpretations of the law' (2015: 1). Since the GDPR, DPAs have tended to work more closely due to increased co-operation in enforcement and handling of complaints (Bieker 2016). This paper will focus mostly on the broader 'EU DPA perspective', notwithstanding 'differences in focus, position and strategy' among the different DPAs due to national differences in legal and administrative frameworks (Barnard-Wills et al. 2016: 596) or area-specific perspectives, such as those of DPAs in post-communist contexts (Svenonius and Tarasova 2021).

Given the important role of DPAs in protecting the fundamental rights and freedoms of citizens in the democratic states of the EU (GDPR Recital 2), the aims of this paper are: (1) to gain a closer understanding of what DPAs consider those threats to be; (2) to understand which solutions are prioritised by DPAs to mitigate those threats; and (3) to identify the *political rationalities* of these solutions. *Political rationalities,* a concept from the post-structuralist school of governmentality studies, can be described as a way of thinking which makes an object or domain accessible to governing interventions (Miller and Rose, 2008). Political rationalities are not just responses to an external problem, but rather constitutive of the problem as such (Bacchi and Goodwin, 2016). Thus, from a governmentality perspective, as the EU and other regimes struggle to make data protection a governable domain, prevailing

political rationalities will shape, steer and direct what the 'problem(s)' of digitalisation (and data protection) regulation is/are represented to be. Understanding 'problem representations' (Bacchi 2012) is useful for identifying political rationalities and the political effects of regulatory and policy solutions.

By identifying these rationalities, we aim to shed light on the tension between the EU's dual (and at times conflicting) goals of digitalisation and the protection of democratic rights and freedoms. We consider the post-structuralist perspective of governmentality and the critical tool of Carol Bacchi's (2012) 'What's the problem represented to be?' (WPR) approach to offer valuable insights into the data protection landscape with respect to how the GDPR is 'made' at the level of implementation. The paper will first discuss governmentality studies of digitalisation, data protection and AI regulation; second, outline the theoretical and methodical approach which draws on governmentality studies and Carol Bacchi's What's the Problem Represented to Be? (WPR) approach; third, present the views of DPAs on the most pressing threats to democracy and our analysis of DPAs' solutions to those threats and fourth, discuss the results.

Governmentality studies of digitalisation, data protection and AI regulation

This section of the paper will first discuss scholarship utilising the governmentality lens or 'toolbox' (Walters 2012) in relation to broader discussions of digitalisation before discussing governmentality approaches which have addressed the field of data protection and AI specifically. Governmentality has been applied as an analytical lens to digitalisation and the way in which we are governed by algorithms. Rouvroy's (2020: 1) conceptualisation of 'algorithmic governmentality' is a process of governing uncertainty through the quantification of the social and the political. As a result, we govern uncertainty through algorithms, rather than politics, law or social norms. This is relevant to discussions of digitalisation regulation insofar as the representation of algorithms in policy discourse as a neutral means to 'achieve' effective or efficient outcomes and can mask what may in fact be highly political decisions, such as decisions governing access to resources or services (Crawford 2021). Amoore (2013) has explored the implications of such 'techniques of calculation' in relation to risk and security practices and the effects of these techniques on the political aspects of what they make possible, and what they exclude. A comprehensive discussion of the concept of algorithmic governance by Katzenbach and Ulbricht (2019) builds on the idea that 'digital technologies structure the social in particular ways'. They argue that the concept is contested and show how it has been used in different sets of literature and disciplines. The application of a governmentality framework to the 'ethics discourse' in AI policy highlights ways in which ethics operates as a 'de-politicising tool' (Rönnblom et al. 2024). Importantly, what governmentality studies share is a de-shrouding of political aspects of the digital and digitalisation policy.

The field of data protection regulation has garnered significant scholarly attention, including from post-structuralist perspectives. Manokha problematises the GDPR's relationship with the current political-economic order and understands the GDPR as 'an instance of neoliberal governmentality' (2023: 6). Manokha argues that the GDPR, whilst promoting individual data ownership, simultaneously facilitates the commodification of personal data. This duality underscores a neoliberal approach whereby regulatory frameworks create markets for personal data while shifting responsibility of data protection onto individuals (2023). Bellanova's (2017) study utilises a governmentality framework to show how digital data is governed through the lens of data protection. Bellanova argues that data protection's two-fold approach aims for people to 'take control of their data' on the one hand, whilst exploiting the social and economic opportunities of data on the other. This means that data protection 'participates in an internal critique about the least intrusive and yet more productive forms of data-driven governance' (2017: 330). More specifically, Bellanova investigates Privacy Impact Statements as a governmental technology, and how they can lead to shutting down possibilities for discussion of the political aspects of things like tracking technologies.

Other governmentality studies relating to data protection include a problematisation of the fairness process in the promotion of human rights (Costa 2016) and the use of data-driven disease surveillance and the regulation of risk in an attempt to make uncertain pandemic futures 'knowable, and thus governable' (Roberts 2019). Yeung (2018) describes 'algorithmic regulation' as a new form of social ordering, in which the 'responsibilisation' of individuals and their 'self-governing capabilities' are brought into alignment with a government's political objectives. Padden and Öjehag-Pettersson (2021) utilise Bacchi's (2012) WPR approach to identify 'problem representations' of risk in the GDPR, being (1) 'lock and key' risks, that is, risks to information previously stored in a secure physical space, such as a locked filing cabinet; (2) risks to mutable norms including fundamental rights, well-being and public interest; and (3) the risk to the economy should personal data not be allowed to flow freely. They find that the GDPR's representation of 'well-being' and 'public interest' privilege economic understandings of these concepts.

Theoretical and methodological approach

As a school of thought, governmentality offers a range of analytical categories for analysing how governing is accomplished in various ways. Following Walters's (2012)

suggestion to treat this toolbox of concepts and principles creatively rather than dogmatically, this article will limit the governmentality analysis to a study of political rationalities in the governing of data protection. To do this, we will engage Carol Bacchi's (2012) 'What's the problem represented to be?' (WPR) approach to identify 'problem representations' in the DPA's stated policy solutions. The WPR approach is a post-structural analytic strategy which allows for the interrogation of policies with respect to how they constitute the problem(s) they propose to solve (2012: 1). Within these 'problem representations' are constructions of reality to which a policy responds. The 'claims to truth' built into these representations underpin the practices arising out of them which, in turn, 'govern' us (Rabinow in Bacchi, 2012: 3). The 'problem representations' we identify will then be interrogated to determine their 'political rationalities'. Political rationalities can be understood as the underlying, internal logic that must be in place in order to problematise a given domain in a particular way and not another.

Foucault argues that to govern is a practice nested in discursively produced mentalities or forms of thinking and ways of representing truth: 'For Foucault, power relations cannot be established, maintained, extended, resisted or mobilised into action, or given material form, without the mediation of discourse' (Doherty 2007: 195). Governmentality scholars are therefore generally interested in how certain domains of reality become the object of rule and how they become the target of programmatic thought that renders them amenable to intervention (Bacchi & Goodwin, 2016; Walters, 2012). To make political rationalities visible, scholars may ask 'what forms of thought, knowledge, expertise, strategies [and] means of calculation' (Dean, 2010: 42) are nested in the ways that rule is articulated? Thus, according to Bacchi and Goodwin (2016: 42) political rationalities are 'the rationales produced to justify particular modes of rule' and they function as ways that make any form of activity thinkable to both rulers and the ruled. These diagrams of power 'draw upon the theories, ideas, philosophies, and forms of knowledge that characterise our intellectual heritage' (2016: 43).

In this article, we utilise the WPR approach in a governmentality analysis on interviews with the heads of 18 EU and EEA DPAs or their delegated senior representative (see Table 1). Our methodological approach is as follows. First, we present the views expressed by the DPAs about what they consider to be the key threats posed by digital technologies to democratic rights and democratic systems of government. Given the role of DPAs in protecting fundamental rights and freedoms, we consider DPAs' views on what this means to be a valuable insight. For the purpose of our analysis, these views can be considered the DPAs' 'problem statements'. Second, we asked DPAs how to best mitigate these 'problems' and from this, we recorded their 'stated solutions'. We then analysed these solutions using the WPR approach to identify their 'problem representations' (Bacchi and Goodwin 2016: 20–21). On the basis of these problem representations, we then identified the political rationalities or ways of thinking which enable data protection solutions to be problematised in these particular ways.

A total of 18 Supervisory Authorities have participated in this study. Requests for an interview were sent to all 34 DPAs in the EU/EEA as well as to the European Data Protection Supervisor (EDPS). Eighteen Supervisory Authorities agreed to participate, including the EDPS. Table 1, 'Interview Data Overview', provides a list of the Supervisory Authorities involved in the study, the format via which they responded, interview length and the position of those interviewed. Data Protection Authorities were asked a set of common questions which included what they consider to be their greatest achievements, where they would like more power, their most significant challenges in the coming two to three years, what they consider to be the greatest risks in relation to democracy and how they propose those risks be mitigated. They were also asked if 'mass surveillance' was a concern of their DPA. The interviews were semi-structured which allowed for follow-up questions.

In performing the analysis, we coded the material in steps. First, we identified the set of problems or challenges as identified by the DPAs when working with data protection (i.e., their stated problems). Second, we coded the stated solutions to these problems as identified by the interviewees. Third, we identified and coded the prevailing political rationalities underpinning these solutions, that is, the rationalities governing data protection as articulated by our participants. Our analytical procedure may be described as abductive as we moved back and forth between theoretical assumptions and empirical data (Mason 2018: 228). Coding, thematic reconstruction and general analytical work were conducted with the aid of the QSR Software application NVivo for qualitative data analysis (released in 2018). Of the DPAs not interviewed, two cited a lack of resources, two expressed interest but we were unable to find a suitable time and 12 did not respond. In order to provide anonymity, DPAs have been allocated a random number for the purpose of referencing their comments in analysis and discussion.

It is worth noting that this study is concerned with identifying overarching political rationalities that steer the 'making' the GDPR by policy practitioners, rather than being a comparative study of DPAs' similarities and differences with respect to policy implementation. We experienced 'code saturation' (Hennink et al. 2017) after around seven interviews in relation to broader questions about how to mitigate democratic threats. Questions about individual aspects of their respective jurisdictions were designed to draw out different approaches due to social, cultural and institutional norms. For example, not all countries permit their DPAs to levy fines against other government agencies. Limitations of the study can be said to relate to comparative aspects among DPAs given that not all DPAs were interviewed. Whilst such differences are

Table 1. Interview data overview.

Supervisory Authority	Date	Format	Interview length	Participants
EDPS	19.3.23	Video conference	1 h	European Data Protection Supervisor
Germany	27.11.22	By telephone	1 h	Federal Data Protection Commissioner
Italy	1.12.22	Video conference	1 h	Commissioner & Senior Legal Counsel
Poland	28.11.22	Video conference	1 h, 30 min.	Advisor to the President of the Office of Personal Data Protection
Sweden	10.5.23	In person	1 h	Commissioner
Greece	12.3.23	Video conference	1 h	Commissioner
Hungary	22.6.23	Video conference	1 h	Vice President and Senior Officer
Austria	14.11.23	Video conference	45 min	Deputy Head
Bulgaria	8.12.22	Video conference	1 h	Head of International Cooperation & Development
Norway	7.9.22	Video conference	1 h	Senior Advisor, Section for Policy Analysis
Slovenia	13.12.22	Written response	n/a	Commissioner
Lithuania	6.12.06	Written response	n/a	Commissioner
Estonia	13.10.22	Video conference	1 h	Foreign Co-operation Advisor
Cyprus	23.11.22	Written response	n/a	Commissioner
Luxembourg	12.6.23	Video conference	1 h	Commissioner
Malta	23.11.22	Video conference	1 h	Commissioner & Senior Legal Counsel
Iceland	22.5.23	Video conference	1 h	Commissioner
Lichtenstein	6.12.22	Video conference	1 h	Commissioner

interesting, this paper is most concerned with where political rationalities underpinning common solutions identified by DPAs to mitigate threats to democracy align or diverge.

Analysis: Challenges, solutions & rationalities

We will now present the results of the interviews and our analysis. First, we will outline what DPAs considered to be the greatest challenges posed by emerging technologies to democratic rights and freedoms. We will then present our analysis of the solutions described by DPAs to mitigate these challenges with respect to their political rationalities.

Threats to democracy as identified by DPAs ('problem statements')

Data Protection Authorities identified a range of potential threats to democratic rights and freedoms arising from digitalisation practices, including: the manipulation of voters in ways akin to the Cambridge Analytica case (Cadwalladr and Graham-Harrison 2018); the erosion of rights in periods of crisis, such as during the Covid-19 pandemic or times of heightened security threats; the potential of AI to erode data protection principles such as data minimisation and purpose limitation (being principles intended to protect the right to privacy, itself an enabler of other rights); the use of profiling to try to manipulate people to behave in certain ways (such as in advertising); the facilitation of polarised debate and hate speech due to algorithmic choices in content delivery; the use of spyware, such as Pegasus, by governments to spy on human rights activists, journalists and political leaders (Corera 2021); the increased potential of governments to categorise people due to the ongoing digitalisation of public services; risks to human rights posed by the combination of profiling and automated decision-making; and broader 'chilling effects' of digitalisation on the exercise of democratic rights and freedoms.

We have chosen to focus on the three most salient themes raised in relation to protecting democratic systems of government and democratic rights and freedoms, being: (1) election interference; (2) automated decision-making; and (3) chilling effects. A feature that these share, along with most of the concerns raised above, is the use of profiling to categorise people and generate inferences which are then used to predict people's likes or dislikes, opinions, psychology and future behaviour. This newly created piece of information, the 'profile', can then be used to make decisions (including automated decisions) about a person or group of people, or to prompt or 'nudge' people to act in certain ways (Gandy and Nemorin 2019). Whether derived from a simple correlation, a complex algorithm or AI, profiling lies at the heart of most of the concerns raised by DPAs about the potentially anti-democratic effects of digitalisation. We will now outline the perspectives of DPAs in relation to these three themes.

Election interference through online manipulation. Manipulation of people through targeted political advertising using big data, profiling and AI was the concern most raised by DPAs when asked what they consider to be the greatest threats posed by digitalisation to democracy. Cambridge Analytica was usually the first example provided by DPAs when asked what they consider to be among the biggest risks posed by digital technologies to democracy:

> Cambridge Analytica…was the use of personal information through social media which had an effect on democratic rights as well. So in my view, I think that we as DPAs have to be careful when we deal with these Big Tech companies in particular, social media companies, because it is not only the privacy policies or the data protection policies which we have to see, or the processing activities at face value, but we have to dig deeper and delve deeper into those black boxes which contain the algorithms and on the basis of which they are able through AI….they are able to collect the information indiscriminately and perhaps use that data to achieve something, you know? Now whether that something is good, or not, that has to be seen. But we have seen cases where that information has been misused in order to achieve an ulterior motive (DPA7).

When citing Cambridge Analytica as an example, DPAs emphasised that the protection of privacy is very much intertwined with the protection of democracy. They generally considered political micro-targeting and the attempted manipulation of voters, whether performed legally or not, to be problematic:

> The bad use of AI systems… to collect and process data – is a big concern for us if these are used with an intention to manipulate the political behaviour of people. If they target the vulnerable, if they abuse the technological capabilities to direct political evolution. Yes, we consider it as a threat to democracy. We have to prevent this, to form an environment that expels such (DPA14).

If the personal data used in cases of political micro-targeting can be shown to have been obtained illegally, such as without explicit consent or without being in the 'legitimate interest' of a business (Article 6), DPAs have a more straightforward case against the data processor. As one DPA put it, although political parties have a legal basis under Article 6 to collect certain information from their members, they do not have a legal justification to collect much more detailed information about their members' habits, such their shopping patterns, online browsing history, interests, psychographic profiles, the music they stream, films they watch and so on (DPA1). However:

> [W]hat they do is they buy data from someone else who stores that data either legally or illegally, but that's not their problem. So they buy it – of course, they do not have a justification for doing it, while that – that's the problem. And if this principle were respected thoroughly by all these companies, we wouldn't have these problems (DPA1).

So even in cases where there is a clear violation of the GDPR, the deliberate concealment of illegal processing makes it difficult for individuals or DPAs to be aware of it in the first place.

One DPA illustrated a case of profiling for political micro-targeting purposes involving Austria Post in 2019. This government-owned company collected and processed personal data to predict the political opinions of residents in Austria, which it then sold to political parties and other entities for purposes of direct marketing on the basis of these predictions. As a result, the Austrian DPA had to deal with many complaints because 'a lot of people were unhappy with this because of the political opinion that they *apparently* had according to the calculations of the Austrian postal company' (DPA6). Even when performed with consent, DPAs were very sceptical towards political micro-targeting as a fair and transparent process. 'Cambridge Analytica was not only illegal, it was *unethical*, since even if it had been possible to avoid that legal issue I think it's a very good example of unethical behaviour' (DPA2). Another DPA described the Cambridge Analytica case, along with Pegasus Spyware, as an example of the dangers of mass surveillance: when it is 'clandestine' and we are unaware 'that somebody else is making a kind of surveillance for other purposes… this is really dangerous, it is dangerous for a democratic system because it can influence us [without us knowing]' (DPA14).

Anti-democratic and discriminatory effects of automated decision-making. Automated decisions, both wholly and in part, were criticised by DPAs in relation to their potentially anti-democratic, discriminatory and controlling effects. For example, DPAs expressed concerns about the anti-democratic effects of 'decider algorithms' in relation to news feeds and highlighted the potential of these types of automated decisions to promote the polarisation of debate and fracturing of public opinion:

> What we see in Europe and in many Western countries is that [people] are more or less questioning the government, they question the state institutions, and I think this can be a very dangerous development because if you do not have a broad societal, how should I say, consent on how a state should work, if you do not have broad consent on how democracy should work and broad societal consent on the plurality of the political system I think it can be a very dangerous development (DPA13).

They also expressed concern about the potentially discriminatory effects of automated decisions in both public and commercial service delivery. For example, profiling may determine the types and prices of products a person is offered, or is not offered, online. The AdTech industry was also singled out as an area of concern for practices such as real-time bidding and other uses of personal data to cajole, nudge or manipulate. One DPA conjectured that the GDPR renders the entire AdTech industry illegal: 'The entire system is a data breach, basically' (DPA5). Given this assessment, the same DPA observed that the consequences of enforcing the GDPR to its full extent to be extreme, as this would render industries like the Adtech sector non-existent:

> The consequences of enforcing the GDPR to its full effect has *enormous* consequences for how we have constructed our digital global world, and I guess some DPAs probably, and most politicians, see their job as being pragmatic, as finding the best balance, and some believe it is too important to negotiate (DPA5).

Automated decisions were also criticised for the way in which they can unfairly govern the behaviour of people, especially workers. One case was of a food delivery company whose algorithm sacked a delivery worker who had been killed the previous day when delivering food orders on his bicycle:

> [The company used] very detailed algorithms for the management of the clients' orders and also for the, let's say, attribution [of performance indicators] to the different workers who deliver food or other products, at times with very strict parameters which have been questioned by our authority in terms of discrimination and the dignity of the worker (DPA15).

Although the head of the company was quoted in the media as stating 'It's not the algorithm that makes you run', the way in which the algorithm was conceived obliged the worker to perform in a particular way, and the example 'shows the impact on real lives of individuals' (DPA15). The use of AI in automated decisions was seen as likely to push the boundaries of data protection principles because it challenges 'the principle of data minimisation and proportionality, as AI generally involves processing vast amounts of data. Also relevant are concerns in relation to profiling and automated decision-making [and the] accuracy of data that is being processed by AI applications' (DPA12).

Chilling effects of digitalisation on liberal democracies. Several DPAs spoke about the 'chilling effects' of digitalisation on democracy: 'Chilling effects are promoting slow change in democratic states. A slow change, but a change nonetheless. So data protection is not only protecting individual rights but the very stable structure of the society itself' (DPA3). Digitalisation was recognised as a challenge in and of itself, given the uptake of a constantly growing array of technologies with in-built surveillance mechanisms, such as 'smart' homes, vehicles and surveillance cameras, and the enormous increase in the processing of personal data associated with these new applications. Digitalisation and AI were considered to promote 'function creep' (DPA3, DPA10, DPA12), that is, 'the expansion of a system or technology beyond its original function' (Koops 2021).

The surveillance aspects of our current form of digitalisation were also linked to chilling effects because they erode the willingness of citizens to exercise their democratic rights and freedoms:

> Digitalisation is linked to chilling effects. If others are collecting your data and judging what your chances are to get a contract, be accepted when entering an office building or the level of risk you are perceived to pose to police or other security forces. So every technology of identifying, of categorising people, that's not just video surveillance, but it's audio, it's the way you move or things like this, is a threat to the idea of free movement and free speech…. You always have to look out if someone is trying to interpret or judge the things you do or don't do. And you have to be aware that you could be identified – that the offers made to you are tailored, but not tailored to your own good but to the ones who are collecting the data, and you can be taken out of getting an offer because you are identified as a group member, of a group which is less interesting for business (DPA3).

Digitalisation was itself thus linked to function creep and an exacerbation of chilling effects.

Given the link between chilling effects and mass surveillance practices (by governments and private companies alike), we asked DPAs whether 'mass surveillance' was a concern of their agency. When asking this question, mass surveillance was not defined by the interviewer. Some DPAs simply answered 'No'. Of these, two referred back to the complaints process as the mechanism determining matters of concern, with one stating: 'My office has not received any complaints in relation to this issue (DPA17)', whilst another response was more tentative, acknowledging that whilst they were not aware of any specific cases, it still might occur (DPA7). Some defined mass surveillance narrowly in their response, as indiscriminate surveillance by governments of their populations, which is not permitted in the EU (DPA13). Others selected examples of surveillance they saw as particularly dangerous for democratic systems of government, such as the cases involving Pegasus Spyware and Cambridge Analytica (DPA14). Other DPAs considered monitoring for mass surveillance an explicit concern of DPAs:

> Mass surveillance entails monitoring of large number of individuals and therefore usually is a concern of a data protection authorities, as it entails processing of large quantities of personal data of the monitored masses of individuals. Especially when modern ICT means are used for surveillance, many data protection issues emerge, and the principles of data protection must be respected: the data must be processed lawfully, the principles of data minimisation, transparency, fairness and security must be respected. The data controllers must develop a data protection impact assessment and consult with the data protection authority (DPA12).

Among the DPAs which criticised the current model of digitalisation in its entirety for its surveillance aspects, one argued that people have been misled to believe that surveillance techniques need to be central to the entire digital ecosystem – but that this does not have to be the case: 'Some people, they do not want to be under that surveillance but somehow they accept it because somehow, some people, even journalists, tell people that this kind of data collection is a *must* with digitisation' (DPA3). Another DPA said that in their country, trust in private companies was generally high, and that whilst the structure of surveillance capitalism was an issue for society, it is not something people consider when choosing a service (DPA10). The challenge for the future was described as how to reap the benefits of digitalisation without surveillance aspects such as categorisation:

> There is a round-the-clock surveillance of everything you do, and do not, and how you feel and how you act, and what is different to other days, and probability, you are brought into groups of people, and they try to extrapolate your behaviour to new questions, so to really get back the freedom and the civil rights for citizens in the digital era. So cloud computing, the internet of things, and every week there is new knowledge coming on the market that has to be investigated: what does that mean for the basic rights of European citizens? (DPA3)

Another DPA compared the practices of private companies in the EU to those of the Chinese government, which is known for its state-based social scoring system:

> We do not have the Chinese state that collects all that data but if we take together all the data that is collected by all the different private companies and as we know, many of them are linked… so I'm not sure whether the Chinese state has more data on its citizens than these private companies. So, it's just that the difference is that the state uses these data for different purposes (DPA2).

Whereas China is often raised as a spectre of what EU countries are not, the suggestion is made that we already have systems akin to social scoring regimes in China, but with private sector operators at the helm, rather than state agencies. Importantly, chilling effects on democratic freedoms can be produced by both state and private entities and can undermine important features of democracy such as political participation. A reluctance to participate was then linked to the potential for EU countries to become less democratic over time (DPA3).

Solutions identified by DPAs ('solution statements'), their 'problem representations' and political rationalities

Having recounted the views of DPAs on key challenges posed by digital technologies to democracy, we now turn to the ways in which DPAs seek to mitigate these threats. What tools do they reach for to deal with these? According to DPAs, risks to democratic rights and freedoms were considered best addressed through *ex officio* activities such as raising awareness among all parties involved in the sharing, collection and processing of personal data. Other factors considered important in relation to minimising risks to democracy included better transparency, codes of conduct and harmonisation of data protection practices across the EU. Data Protection Authorities also considered the principles of fairness (GDPR Article 5(1)(a)) and the principle of proportionality (GDPR Recital 4) paramount, that is, that the fundamental right to the protection of personal data and to privacy needs to be 'balanced' with other rights. They reinforced the importance of 'trust', considered to be rooted in transparency

(DPA10). In analysing the stated solutions to democratic threats as identified by DPAs, we identified their 'problem representations' as a means to then identify the political rationalities underpinning them. By identifying these rationalities, we can better understand what is considered possible and what is excluded in the delimitation of data protection solutions to these challenges. Whilst it was not surprising that DPAs reached first and foremost for remedies available to them in the GDPR, what was interesting was where DPAs were more creative in working around the GDPR's limitations with respect to protecting democratic freedoms.

Responsibilisation of the individual through the complaints process. Data Protection Authorities turned to the GDPR's complaints process as a solution to the anti-democratic effects of profiling by Big Tech and governments. The 'problem representation' of this stated solution, that a complaints process can mitigate the anti-democratic effects of profiling, implies that it is the responsibility of the individual to instigate an investigation into a suspected data breach. Whilst this may be effective in dealing with 'lock and key' risks such as to the personal information of a specific individual, it precludes investigations into more general anti-democratic effects. Indeed, the work of DPAs is principally concerned with resolving complaints made by individuals ('data subjects') about violations of the GDPR with respect to their personal data (Recital 122). Individual complaints are rarely, if ever, about democracy, as the complaint needs to relate to the individual (DPA10, DPA5 and DPA7). Some cases do relate to democratic freedoms, such as the case of Clearview AI (DPA18), or strategic complaints lodged by civil rights organisations such as the European Center for Digital Rights (also known as NOYB) (DPA13) but they need to relate first and foremost to illegal processing of the personal data of a specific individual. Reporting data breaches, it should be noted, is also the responsibility controllers of data processing operations (Article 33).

Either solution, requiring individuals or data controllers to take responsibility for lodging a complaint or reporting a breach or unfair practice nevertheless excludes the possibility to make complaints that might redress some of the concerns raised by DPAs concerning chilling effects or polarisation. For example, there is no legal recourse to not *feeling* such as exercising your democratic rights or expressing a political opinion because you *suspect* your comments will be somehow used by an unknown party, yet such suspicions produce anti-democratic effects. Furthermore, the GDPR excludes the possibility to complain about being categorised and discriminated against based on profiles developed using anonymised data. The work of DPAs in relation to upholding democratic principles and fundamental rights and freedoms therefore often falls to their efforts in an *ex officio* capacity, that is, outside the complaints process. The extent to which DPAs are engaged in *ex officio* activities can vary considerably, depending upon their resources and each agency's strategic priorities.

Awareness and individual responsibilisation. When asked how to best mitigate threats to democracy, DPAs turned to awareness-raising among individuals and society generally as a favoured solution. The 'problem representation' of this stated solution, that awareness can mitigate the anti-democratic effects of digital technologies, implies that awareness, whether individual or collective, can somehow minimise or prevent people from being manipulated by the influencing efforts of those who using profiling for the very purpose of manipulation. Data Protection Authorities expressed the view that increased awareness of one's rights is an essential precursor to an individual taking steps to redress any suspected transgression under Article 6 of the GDPR, which sets out what constitutes lawful data processing. Notably, when DPAs were asked to describe their 'biggest wins', increased societal awareness about data protection was named by every DPA interviewed as among their most significant achievements, reflected in an increased number of complaints. However, despite the obvious merits of awareness, especially in the absence of other measures, awareness as a solution still serves to 'responsibilise' the individual upon whom the burden is placed *to be aware*.

This is particularly problematic in instances where data processors or controllers are concealing the fact that personal data has been obtained illegally, or when algorithms used to make decisions are opaque to the user. Whilst decisions such as what content to show a YouTube or social media user may not have any significant legal effects for a particular individual under Article 22, the decisions made across the board for *all* users may have a collective impact on popular opinion. Despite the GDPR's mandate to protect democratic rights and freedoms, it is unrealistic to expect DPAs to mitigate more general, societal 'chilling' or polarising effects of digitalisation without a legal basis to do so. That said, many of the DPAs interviewed care very much about these issues and attempt to mitigate them nonetheless, by raising awareness among their countries' politicians and civil servants and by expressing the views of their authorities in public debate.

Awareness was also raised by DPAs as the most significant path to ensuring people exercise their rights in relation to automated decision-making. If people are not aware, for example, of their right not to be subject to a fully automated decision with a potentially significant effect under Article 22, 'such as automatic refusal of an online credit application or e-recruiting practices without any human intervention' (Recital 77), they will not exercise their right 'to obtain human intervention' (Article 22). One DPA illustrated the positive effects of the GDPR on newly emerging AI

technologies: 'Increased awareness has led people to realise that they can use their rights under the GDPR such as their right of access and the right to delete unlawfully processed information in sectors without similar protections, such as has been the case in relation to credit worthiness assessments' (DPA14). This can now be seen to be happening in relation to AI due to applicable laws in data protection, such as 'the right not to be subject to automated decisions, which made it a little spontaneous and natural to refer to data protection rules when dealing with artificial intelligence, [although] artificial intelligence has a wider range of implications that we should consider' (DPA14).

Another aspect of awareness-raising by DPAs occurs in relation to the presentation of alternative solutions to both their governments and the public. In the interviews, for example, some DPAs raised concerns with the fundamental construction of digitalisation as it is unfolding in our societies today, such as its unnecessary reliance on surveillance practices (DPA3). This, along with the assertion that the AdTech industry is likely illegal in its entirety (DPA5), is examples of a much more political form of awareness-raising and acts of resistance taken on by some DPAs. One could speculate that such comments might stem from a frustration arising when tasked with a mandate to protect democratic rights within a system which permits the very practices deemed to threaten them. In this respect, DPAs provide an important critical voice in drawing political attention to these issues.

Transparency and individual responsibilisation. Transparency, like awareness, was a key solution for DPAs and linked to other principles such as fairness, as well as being necessary to build trust: 'It's possible that sometimes practices are not transparent enough to make you understand what goes on. But they should be, because transparency is one of the most important principles about data protection. Sometimes it's not completely upheld by companies' (DPA7). It was also thought that transparency would become an increasingly important principle in relation to AI (DPA 18). Whilst transparency is considered by some to be the most important aspect of data protection (DPA1), transparency in AI is seen as something which will become increasingly challenging (DPA7). The implications of the 'problem representation' of transparency as able to mitigate anti-democratic effects is twofold. First, it implies that it is the responsibility of the data controller to provide information 'relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12)'. This includes providing the information orally if requested (Article 12). The second aspect of this 'problem representation' is the assumption that being transparent about purposes such as profiling with the intention to target and manipulate a person will somehow prevent any manipulative effects intended by the controller. Whilst the requirement of transparency at first appears to responsibilise data controllers, responsibility is still shifted to the individual who is usually required to read and understand reams of complex legal texts. Placing responsibility upon individuals to interpret such information and then consent to it in an environment where 'stealth' is a corporate objective is biased from the outset and favours well-resourced industries.

Transparency is linked to consent as it is the explanations about how data will be processed to which users agree, such as to tracking what they do across other websites or sharing their data with other companies, such as data brokers. Consent must be 'freely given, specific, informed and unambiguous' (Article 4(1)). Data Protection Authorities explained their own hesitancy about pushing consent as a solution given it was 'too bureaucratic' or 'was another heavy aspect for the individual, for the companies, for enterprises, or the public bodies' (DPA15). Indeed, mechanisms for obtaining consent have been critiqued from the designs of pop up notices intended to 'nudge' people into agreeing to be tracked (Utz et al. 2019) to the lack of 'true consent' being obtained by companies through box-ticking mechanisms (Breen et al. 2020). One DPA considered that 'the consents used today cannot comply with what the law says so in my view most of the data practice going on is unlawful' (DPA5). Notwithstanding arguments over the form consent should take, consent places responsibility for the acceptance of tracking squarely on the shoulders of the individual. If an individual continually agrees to share their data, 'in the end, ok, the user loses his power, yes, of their data' (DPA18).

Concluding discussion

We now provide a discussion of the political rationalities underpinning data protection solutions which aim to mitigate the anti-democratic effects of digitalisation. We argue that individual responsibilisation aspects of policy solutions such as complaints processes, awareness, transparency and consent operate through 'control constructs', or the dynamics of perceived threats to personal control, identified more broadly as a feature of neoliberal governance 'which tries to render the social domain economic' (Pyysiäinen et al. 2017). This responsibilisation serves to create a subject who is seen as having 'free choice' (DPA8) through 'control over their own data' (DPA1) yet in being afforded these things is made an active agent in the protection of their own, and society's democratic rights, which is a responsibility one could alternatively see as being that of the collective whole. This places a cumbersome expectation upon individuals that they can feasibly manage an increasingly unmanageable and oftentimes invisible swathe of surveillance practices. Sometimes these have very personal implications, such as being

flagged by an algorithm as unlikely to succeed in a particular job or in repaying a loan. In other cases, the democratic freedoms of *every* individual, such as freedom of movement or of association, may be at risk of being gradually eroded. In the section which follows, we emphasise that the policy solutions to 'non-economic' problems, such as the protection of democratic rights and freedoms, fit within Foucault's conception of neoliberalism as a governing rationality, being 'a specific way of organising social relations on the basis of a rationality dictated by the market' (Lorenzini 2018: 155). We argue that individual responsibilisation serves to depoliticise data protection solutions and excludes more collective alternatives.

Responsibilisation of individuals in data protection regulation is by no means an isolated case but is an existing theme in governmentality literature (Rose and Miller 1992) and is connected to advanced liberalism (Juhila et al. 2017). According to Wendy Brown, individual responsibilisation is a key mechanism through which neoliberalism operates and in this 'responsibilised turn', '*homo oeconomicus* as human capital leaves behind not only *homo politicus*, but humanism itself' (Brown 2015: 41–24). In addition to the privileging of economic progress through a political rationality of individual responsibilisation, the GDPR is specifically purposed with protecting the EU's economic development by ensuring the 'free flow' of data. This, in conjunction with the effects of individual responsibilisation, enables the co-existence of anti-democratic surveillance practices alongside the regulatory measures said to curb their effects.

Solutions not based on individual responsibilisation raised by DPAs included industry codes of practice as a means of creating transparency and therefore fairness (DPA14). Whilst these represent industry rather than individual responsibility, they nevertheless serve to strengthen economic imperatives and the privileged position of business interests in the data protection landscape. For example, the 'legitimate interests' of business are a legal basis for processing data under Article 6, and these include 'direct marketing purposes', as long as they do not override a data subject's fundamental rights and freedoms (Recital 47). As Bellanova (2017: 338) points out in relation to the European Commission's 2009 Privacy Impact Assessment Framework for the use of Radio-Frequency Identification (RFID) tags, procedures reliant upon industry self-assessment can exclude wider public consultation. In so doing, what should be *political* decisions, that is, the permitting of large-scale surveillance via RFID cards utilised across multiple industries, such as transport cards, clothing items and other consumer products, are determined – by private sector operators with an economic interest in their use – to be *technical* problems.

In addition to placing a burden on the individual, the assumption that transparency and awareness are effective tends to play down the effects of the processes in question. Implicit in transparency and awareness as policy solutions is the presumption that just *knowing* about the potential effect of a process such as profiling or micro-targeting, or that a particular automated decision may have had a significant effect on you, can somehow stop its effects. Awareness and transparency as solutions therefore help to preclude alternative solutions such as the outright banning of practices deemed anti-democratic. At the same time, awareness and transparency as 'solutions' enable continued profiteering from the use of surveillance practices, whilst appearing to make efforts to curb their negative effects. This view is apparent in the reasoning behind the EU's Regulation on the transparency of political advertising (European Union 2024) and the use of targeted 'amplification techniques', that is, advertisements tailored to a specific person or group (European Union 2024). The law does not ban political micro-targeting but seeks to raise awareness on the part of citizens that they are being targeted for the purpose of manipulation. Transparency of this attempted manipulation, as argued in the explanatory memorandum of the initial proposal, will help by 'reducing the possibility of manipulation of the democratic debate and the right to be informed in an objective, transparent and pluralistic way' whilst maintaining the right to freedom of expression by the advertiser (European Commission 2021).

Ultimately, the neoliberal political rationalities governing the GDPR limit the solutions available to policy-makers and to DPAs to mitigate the anti-democratic effects of digitalisation. The GDPR is rendered unsuitable to address broader, societal challenges to democracy because it frames problems and solutions in terms of individual responsibility and economic interest. In this article, we have shown how this 'mismatch' is expressed in interviews with DPAs. Individual responsibilisation, along with the 'bets' placed on big data (Giraudo et al. 2024) by both businesses and governments, leave policy practitioners without the means to cut the head off the snake: DPAs cannot, at least within their current mandate, re-shape the form which digitalisation has hitherto taken. At best, they can attempt to reduce the flow of anti-democratic incursions or be so bold as to suggest the system be reconfigured.

With the free flow of data decided upon as a key means to boost the economy and enshrined as a goal of the GDPR, surveillance practices once ruled as incompatible with democracy are now permitted in the interests of efficiency and economic growth. The transformation of how surveillance has been represented in policy discourse is a process that has evolved over time (Padden 2023) and forms part of a broader 'illiberal drift' in democratic states (Tréguer 2017). In this paper, we have sought to highlight a disconnect between what DPAs put forward as the most pressing challenges facing democratic states and the tools available to them to mitigate them. It will take tremendous resilience and persistence to resist the political rationalities which

shape the current anti-democratic trajectory of digitalisation. The practical implications of reconfiguring our digital future may well appear impractical, but the long-term consequences of *not* doing so are too profound to ignore.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Michaela Padden https://orcid.org/0000-0003-3924-315X

References

Amoore L (2013) *The Politics of Possibility: Risk and Security Beyond Probability*. Durham and London: Duke University Press.

Bacchi C (2012) Why study problematizations? Making politics visible. *Open Journal of Political Science* 2(1): 1–8.

Bacchi C and Goodwin S (2016) *Poststructural Policy Analysis: A Guide to Practice*. New York, NY: Springer.

Barnard-Wills T, Chulvi CP and De Hert P (2016) Data protection authority perspectives on the impact of data protection reform on cooperation in the EU. *Computer Law and Security Review* 32(4): 587–598.

Bellanova R (2017) Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory* 20(3): 329–347. https://journals.sagepub.com/doi/10.1177/136843101667916

Bieker F (2016) Enforcing data protection law–the role of the supervisory authorities in theory and practice. In: *IFIP International Summer School on Privacy and Identity Management*. Cham: Springer International Publishing, 125–139.

Bosco F, Creemers N, Ferraris V, et al. (2015) Profiling technologies and fundamental rights and values: Regulatory challenges and perspectives from European data protection authorities. In: *Reforming European Data Protection Law*. Dordrecht: Springer, 3–33.

Breen S, Ouazzane K and Patel P (2020) GDPR: Is your consent valid? *Business Information Review* 37(1): 19–24.

Brown W (2015) *Undoing the Demos*. Brooklyn: Zone Books.

Cadwalladr C and Graham-Harrison E (2018) Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cave S and ÓhÉigeartaigh SS (2018) An AI Race for Strategic Advantage: Rhetoric and Risks.Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society.

Corera G (2021) Pegasus Scandal: Are we all becoming unknown spies? BBC. Web. https://www.bbc.com/news/technology-57910355

Costa L (2016) Data protection law, processes and freedoms. In: *Virtuality and Capabilities in a World of Ambient Intelligence. Law, Governance and Technology Series*, Vol. 32. Cham: Springer.

Crawford K (2021) *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven and London: Yale University Press.

Dean M (2010) *Governmentality: Power and Rule in Modern Society*. London: Sage Publications Ltd.

Doherty R (2007) Chapter 13: Critically framing education policy: Foucault, discourse and governmentality. *Counterpoints* 292: 193–204.

European Commission (2011) Data is the new gold. Speech. Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Data. In: Opening Remarks, Press Conference on Open Data Strategy Brussels, 12 December 2011. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_11_872

European Commission (2020) Shaping Europe's digital future. COM (2020) 67. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067

European Commission (2021) Proposal for a regulation of the European parliament and of the council on the transparency and targeting of political advertising. Brussels, 25.11.2021, COM (2021) 731 final, 2021/0381(COD). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0731

European Data Protection Supervisor (EDPS) (2015) Data protection as a bulwark for digital democracy. Speech. https://www.edps.europa.eu/sites/default/files/publication/15-12-10_edemocracy_en.pdf

European Union (2024) Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (Text with EEA relevance). Brussels: Official Journal of the European Union.

European Union (2016) 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 (General Data Protection Regulation). Brussels: Official Journal of the European Union.

European Union (2021) *Regulation (EU) 2021/0106 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*. Brussels: Official Journal of the European Union.

European Union (2022a) *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*. Brussels: Official Journal of the European Union.

European Union (2022b) *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).* Brussels: Official Journal of the European Union.

Fischer S-C and Wenger A (2021) Artificial intelligence, forward-looking governance and the future of security. *Swiss Political Science Review* 27(1): 170–179.

Flaherty DH (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany*. Sweden, France, Canada, and the United States: UNC Press Books.

Flaherty DH, Agre PE and Rotenberg M (1997) Controlling surveillance: Can privacy protection be made effective? In: *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press, 167–192.

Gandy OH Jr and Nemorin S (2019) Toward a political economy of nudge: Smart city variations. *Information, Communication & Society* 22(14): 2112–2126.

Giraudo M (2022) On legal bubbles: Some thoughts on legal shockwaves at the core of the digital economy. *Journal of Institutional Economics* 18(4): 587–604.

Giraudo M, Fosch-Villaronga E and Malgieri G (2024) Competing legal futures–"commodification bets" all the way from personal data to AI. In: *German Law Journal*. Online: Cambridge University Press, 1–25.

Hennink MM, Kaiser BN and Marconi VC (2017) Code saturation versus meaning saturation: How many interviews are enough? *Qualitative Health Research* 27(4): 591–608.

Jóri A (2015) Shaping vs applying data protection law: Two core functions of data protection authorities. *International Data Privacy Law* 5(2): 133. Oxford University Press.

Juhila K, Raitakari S and Hall C (2017) *Responsibilisation at the Margins of Welfare Services*. London: Routledge.

Katzenbach C and Ulbricht L (2019) Algorithmic governance. *Internet Policy Review* 8(4): 1–18. https://policyreview.info/concepts/algorithmic-governance.

Koops B-J (2021) The concept of function creep. *Law, Innovation and Technology* 13(1): 29–56.

Lasswell HD (1971) Policy problems of a data-rich civilization. In: Westin AF (ed) *Information Technology in a Democracy*. Cambridge, MA: Harvard University Press, 187–197.

Lorenzini D (2018) Governmentality, subjectivity, and the neoliberal form of life. *Journal for Cultural Research* 22(2): 154–166.

Manokha I (2023) GDPR as an instance of neoliberal governmentality: A critical analysis of the current 'gold standard' of data protection. In: *Political Anthropological Research on International Social Sciences*. Leiden: Brill, 173– 218. https://brill.com/view/journals/pari/4/2/article-p173_004.xml?language=en

Mason J (2018) *Qualitative Researching*. 3rd ed. London: Sage Publications Ltd.

Miller P and Rose N (2008) *Governing the Present: Administering Economic, Social and Personal Life*. Cambridge: Polity.

Organisation for Economic Co-operation and Development (OECD) (1971) *Digital Information and the Privacy Problem*. Paris: OECD Publishing.

Padden M (2023) The transformation of surveillance in the digitalisation discourse of the OECD: A brief genealogy. *Internet Policy Review* 12(3): 1–39. https://policyreview.info/articles/analysis/transformation-of-surveillance-in-digitalisation-discourse.

Padden M and Öjehag-Pettersson A (2021) Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR). *Critical Policy Studies* 15(4): 486–503.

Pyysiäinen J, Halpin D and Guilfoyle A (2017) Neoliberal governance and 'responsibilization' of agents: Reassessing the mechanisms of responsibility-shift in neoliberal discursive environments. *Distinktion: Journal of Social Theory* 18(2): 215–235.

Raab C and Szekely I (2017) Data protection authorities and information technology. *Computer Law & Security Review* 33(4): 421–433.

Roberts S L (2019) Big data, algorithmic governmentality and the regulation of pandemic risk. *European Journal of Risk Regulation* 10(1): 94–115.

Rönnblom M, Carlsson V and Padden M (2024) AI and ethics: policies of de-politicisation? In: *Handbook on Public Policy and Artificial Intelligence*. Cheltenham: Edward Elgar Publishing, 123–132. https://www.e-elgar.com/shop/gbp/handbook-on-public-policy-and-artificial-intelligence-9781803922164.html

Rose N and Miller P (1992) Political power beyond the state: Problematics of government. *The British Journal of Sociology* 43(2): 191–224.

Rouvroy A (2020) Algorithmic governmentality and the death of politics. *Green European Journal*. 1–5. https://www.greeneuropeanjournal.eu/algorithmic-governmentality-and-the-death-of-politics/

Simitis S (1983) Data protection – a few critical remarks. *Transnational Data Report* 6(2): 93–96.

Smuha NA (2023) From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence. *Law, Innovation and Technology* 13(1): 57–84.

Svenonius O and Tarasova E (2021) "Now we are struggling at least": Change & continuity of surveillance in post-communist societies from the perspective of data protection authorities. *Surveillance & Society* 19(1): 53–68.

Tréguer F (2017) Intelligence reform and the Snowden paradox: The case of France. *Media and Communication* 5(1): 17–28.

Ulnicane I (2023) Against the new space race: Global AI competition and cooperation for people. *AI & SOCIETY* 38(2): 681–683.

UNICRI (United Nations Interregional Crime and Justice Research Institute) (2013) The PROFILING project. Website: https://web.archive.org/web/20130815105414/http://profiling-project.eu/.

Utz C, Degeling M, Fahl S, et al. (2019) (Un)informed consent: Studying GDPR consent notices in the field. In: Conference: ACM SIGSAC Conference on Computer and Communications Security, London, pp. 973–990.

Walters W (2012) *Governmentality: Critical Encounters*. London and New York: Routledge Taylor & Francis Group.

Yeung K (2018) Algorithmic regulation: A critical interrogation. *Regulation and Governance* 12(4): 505–523.