Technology and Regulation

Legality and Democratic Deliberation in Black Box Policing

Markus Naarttijärvi*

Policing, legality, Rule of Law, technology, black box policing, democracy, surveillance, machine learning

markus.naarttijarvi@umu.se

The injection of emerging technologies into policing implies that policing mandates in law may become mediated and applied through opaque machine learning algorithms, artificial intelligence, or surveillance tools – contributing to a form of 'black box policing' challenging foreseeability and clarity and expanding discretionary legal spaces. In this paper, this issue is explored from a constitutional and rule of law perspective, using the requirements of qualitative legality elaborated by the European Court of Human Rights and the implicit democratic values that they serve. Placing this concept of legality into a wider theoretical framework allows legality to be translated into a context of emerging technology to maintain the connections between rule of law, democracy, and individual autonomy.

1. Introduction

1.1 Governing by, and through, technology

Governing is increasingly mediated through digital technology. This is visible in everyday citizen-government interactions, such as online applications for government benefits, income tax declarations and other common e-government services. The digitally mediated nature of governing becomes even more apparent in the face of algorithmic decision-making, where big data and machine learning form a basis for the application of government power and authority.[1] Moreover, the classification of individuals through the observation of their digital footprints is increasingly establishing itself as a governmental shorthand of power, potentially forming the basis for both coercive actions and lethal force.[2] While often discussed in terms of the potential for interferences with privacy or data protection rights, these developments also challenge more fundamental legal values; given the importance of digital technologies in the current exercise of government power, the technologies themselves become crucial for the analysis of whether or not legality as a basic rule of law value is upheld. Legality, understood here in a constitutional context, implies that the exercise of government power should have a basis in law. In a modern understanding – influenced by rule of law values and human rights adjudication – legality also establishes that this legal basis must reach a certain quality; to ensure the accessibility and clarity of law, enable foreseeability, and limit government discretion.[3] As will be shown, these qualitative aspects of legality, as elaborated most clearly by the European Court of Human Rights, also fulfil other, more implicit but equally important, democratic values.

The hypothesis of this paper is that technology adds obscurity to the exercise of law and government power. This obscurity may in many contexts affect the ability to uphold legality as a rule of law value and as a normative limit to government power. While uncertainty is not uncommon in law, it is traditionally perceived as an issue connected to the clarity of legal rules as such and the often-unavoidable indeterminacies of human language that law is expressed through, or such generalisations that are intentionally included to ensure a certain flexibility.[4] Technology, however, adds a different layer of obscurity as the effect of law and the exercise of government power is mediated through a layer of coded norms, logic and presumptions that are external to law and that may be unforeseeable to both legislators and citizens. Technology, as will be shown, may simultaneously act as a driver of vague or indeterminate legislation and inject indeterminacy into an otherwise clear and foreseeable language of law. This raises issues not only with legality, but also with societal values that legality serves, such as the separation of powers, individual autonomy, and democratic legitimacy.

* Markus Naarttijärvi is an associate professor of law at the department of law at Umeå university, Sweden.

Received 25 June 2019, Accepted 22 Oct 2019, Published: 1 Nov 2019

1 See Andrew D Selbst, 'Disparate Impact in Big Data Policing' (2018) 52 *Georgia Law Review* 109; Mireille Hildebrandt, 'Proactive Forensic Profiling: Proactive Criminalization?' in R Anthony Duff and others (eds), *The boundaries of the criminal law* (Oxford University Press, 2010); Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press, 2018); Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press, 2017).

2 See Kevin D Haggerty and Richard V Ericson, 'The Surveillant Assemblage' (2000) 51 *The British Journal of Sociology* 605; Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Vintage Books, 1995); Paul De Hert and Serge Gutwirth, 'Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power' in Anthony Duff, Serge Gutwirth and Erik Claes (eds), *Privacy and the Criminal Law* (Intersentia, 2006).

3 See further section 3 below.

4 Cf. Timothy AO Endicott, *Vagueness in Law* (Oxford University, 2000) 160–164.

The implications of technology are of particular concern in relation to policing, as a context of government power that is subject to detailed regulation given its implications for individual rights, while it is simultaneously an activity which is characterised by significant amounts of autonomy and discretion for both officers and police authorities.[5] As such, technology can be applied in policing through these discretionary spaces while having significant effects on the exercise of power in practice – creating in effect a form of *black box policing* affecting the ability of both citizens and legislators to understand the scope and impetus of police actions and the role technology has played in shaping them. Policing is also an area subject to intense public and political pressure to 'get the job done', which further incentivises the use of technology to reach efficiency targets.[6] Consequently, policing is an area of law where the implications of technology in terms of mediating law and policy into practical effects for individuals may carry tangible and far-reaching implications. The examples provided in the policing context may therefore illustrate implications of obscurity due to technologically mediated governing for both legality and democracy which are relevant for other contexts as well. It may also lay the foundation for an analysis of how legality as a component of rule of law may be translated into a context of technologically mediated governing to preserve such values that underpin legality.

First, however, something should be said about the term *technologically mediated governing*. I use this term here as a shorthand for a behind-the-scenes normative layer of code and data that change the implications of governing through law and government decisions. There are somewhat similar concepts used by other authors carrying other implications. In his analysis of the role of technology as a tool of governing Brownsword uses the term 'technological management', referring to how technology is used normatively to restrict or reduce existing human possibilities by making rule breaking technologically impossible; a simple example is technologically ensuring that cars stop at red lights rather than relying on norms to encourage or coerce drivers to do so.[7] I use the term technologically mediated governing here to instead signify how the application of a certain technology alters (i.e. mediates) the implications of governing through law, rather than through technology as such. This may in some instances include technological management as conceptualised by Brownsword, however, technologically mediated governing is not dependent on the restriction or reduction of human possibilities through technology itself.[8] In other words, the interest is not so much how technology serves to ensure individual compliance, as how the exercise of government power mediated by technology affects legality. In this sense, I approach the technologically mediated nature of governing from a perspective that is similar to the concept of digitisation as defined by Yoo *et al.* as 'the transformation of existing socio-technical structures that were previously mediated by non-digital artefacts or relationships into ones that are mediated by digitized artefacts and relationships with newly embedded digital capabilities'.[9] This goes beyond the mere technical process of digitisation of analog information and 'involves organizing socio-technical structures with digitized artefacts [and] the reconfiguration of broader socio-technical structures that were previously mediated by non-digital artefacts'.[10] The use of these technologies also implies, as noted by Latour, the mobilisation of 'moves made elsewhere, earlier, by other actants'.[11] This entails that technologies used in policing will effectuate the values, choices, and norms embedded in those technologies at an earlier date. In other words, the mediation of technology will not only alter implications of law through its interpretation into new contexts, or the new possibilities afforded by the technology,[12] but also through a form of normative refraction which occurs as the legal norms interact with the embedded values, choices, and norms of the technology used.

In the rest of this first section, I will underpin the importance of technology as a tool of governing through conclusions drawn in existing research. In section 2, I will point to examples from the policing context where technologically mediated governing challenges legality. These examples will serve as a background for a broader analysis of legality in section 3, first as a more abstract value, then as a normative requirement as applied in the case law of the European Court of Human Rights (ECtHR). In section 4, I will argue for a broader reading of legality which implicitly serves democratic values. Finally, in section 5, I will sketch out an understanding of legality that highlights the importance of upholding both legal and democratic values in the face of emerging technology and provide some tentative recommendations on how to approach its application.

1.2 The importance of features, code, and data

The importance of technology for governing has become apparent since the rise of the network society.[13] As Lawrence Lessig has noted, we embed different values when constructing code and choosing different technological architectures, and the decisions made regarding these same codes and architectures enable control from whatever sovereign that does the coding.[14]

> [I]f in the middle of the nineteenth century the threat to liberty was norms, and at the start of the twentieth it was state power, and during much of the middle twentieth it was the market, then my argument is that we must come to understand how in the twenty-first century it is a different regulator – code – that should be our current concern.[15]

5 Elizabeth E. Joh uses the term 'surveillance discretion' to refer to the far-reaching discretion of the police in deciding who to investigate and focus their attention on. See Elizabeth E Joh, 'The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing' (2016) 10 *Harvard Law and Policy Review* 15, 16. See also Selbst (n 1) 119, who comment that '[p]olice act with incredible discretion. They choose where to focus their attention, who to arrest, and when to use force. They make many choices every day regarding who is a suspect and who appears to be a criminal.'

6 Cf. Lena Landström, Niklas Eklund and Markus Naarttijärvi, 'Legal Limits to Prioritisation in Policing – Challenging the Impact of Centralisation' (2019) *Policing and Society* (online pre-print).

7 Roger Brownsword, 'In the Year 2061: From Law to Technological Management' (2015) 7 *Law, Innovation and Technology* 1, 8.

8 As such, the interest here — to use the same example of the red light — is rather how technology may be used to either identify persons who did not stop at the red light and then use law to sanction them, or more proactively to identify who is more likely not to stop at the red light and then use existing government powers to control or coerce them in their car use.

9 Youngjin Yoo and others, 'Unbounded Innovation with Digitalization: A Case of Digital Camera', 2010 *Annual Meeting of the Academy of Management* (2010) 4.

10 Yoo and others (n 9) 4. As Yoo et al looked at digitisation of products, these artefacts would in this context instead be the digitisation of government powers and methods.

11 Bruno Latour, 'On Technological Mediation' (1994) 3 *Common Knowledge* 29, 52. See also Don Ihde, *Technology and the Lifeworld* (Indiana University Press, 1990) 49, stating that 'for every revealing transformation there is a simultaneous concealing transformation of the world, which is given through a technological mediation. Technologies transform experience, however subtly, and that is one root of their non-neutrality'.

12 Cf. Peter-Paul Verbeek, *Moralizing Technology – Understanding and Designing the Morality of Things* (University of Chicago Press, 2011) 5.

13 For the use of this term, see Jan van Dijk, *The Network Society* (Sage Publications, 2012).

14 Lawrence Lessig, *Code: Version 2.0* (Basic Books, 2006) 77, 114.

15 Lessig (n 14) 121.

Given the importance of architecture, it is, Lessig holds, important not to ignore this type of regulatory modality or accept it as given – rather, it needs to be taken into account in the making of law, and the technological responses to law must be predicted.[16]

In a similar vein, Hildebrandt aptly uses the term *affordances*, borrowed from biology, to explain how 'technologies afford certain behaviours that would otherwise have been impossible, or do not afford certain behaviours that were available before the technology was in place'.[17] From this point of departure, she argues that criminal justice has been afforded a more actuarial approach where the focus is placed on profiling and the characteristics and calculated risk a person represents, rather than the actual actions of that person as such.[18] Such actuarial justice may also be represented by the increased emphasis on intelligence-led policing (ILP), focusing on patterns and predictability rather than approaching crime on a case-by-case basis.[19]

As such, technology will affect *what* law governs, but also *how* law governs. For example, before the advent of digital networking, the idea of massive interception and automated processing of telecommunications was scarcely afforded by the available technology.[20] Given the increased availability of data and the development of processing power and software to automatically process these data, the concept of massive, or bulk, interception has increasingly become afforded by technology, and as such a clear focus of government surveillance efforts and legislation in the last decades. While modern conceptions of terrorism following 9/11 have acted as drivers of this type of surveillance, the interaction between developments in the security paradigm and the technological developments of data processing has acted as a catalyst to enable the rise of the modern surveillance state.[21]

The affordance of new methods of governing within the field of policing brings us to one of the main issues in relation to legality, namely the potential for technological obscurity – i.e. the way the injection of technology can cloud the implications and effects of legal mandates and policing methods, with potential effects for both the accessibility and foreseeability of law.

2. Delineating the black box of policing

As previously mentioned, the hypothesis of this article is that technology adds obscurity to the application of law and government power. In this section, I will establish the further basis for this hypothesis and outline four ways in which technology either expands discretionary spaces in ways that are opaque for persons outside of a police force, or injects obscurity into existing methods of policing, thereby shifting the practical and regulatory environment where police authorities act. This is not an exhaustive list of possible concerns, but represents such areas of concern that have been either highlighted in previous research or that present a *prima facie* challenge to the ideals of qualitative legality, as I will soon describe further.

2.1 Avoiding regulatory negotiation: discrete and direct application of technology

In many contexts, executive agencies and other government organs, including law-enforcement authorities, are dependent on law-makers to arbiter and decide where the interests of public authorities collide with those of private interests or individuals. This is the case when the law requires private entities to assist the police in inquiries or provide material support such as enabling and assisting the police in the surveillance of phone networks. A clear example of this is how the EU data retention directive – while in force – created a responsibility for EU member states to enact legislation which required private telecommunications providers to retain communications data for law enforcement purposes.[22] When enacting these rules, law-makers – and by extension courts – are forced to balance public and private interests, while keeping in mind such constitutional rules and limits that may provide a proverbial thumb on the scale in certain contexts.[23]

The situation is however different when authorities can achieve their aims by more direct and discrete means. Technologies such as IMSI-catchers (a piece of equipment masquerading as a mobile base station, capturing information about nearby mobile equipment) upsets this balance by allowing – in the practical sense – authorities (as well as private parties) to monitor communications and surrounding devices without going through telecommunications providers.[24] The implication of direct and discrete applications of technology is that the very practical need for the legislature to enable the application of a certain technology within government agencies is reduced or eliminated. There are no communication providers to convince or coerce into cooperation when using an IMSI-catcher, as the technology affords direct surveillance to whomever has access to the equipment in question. As such, the nature of the technology in conjunction with efficiency demands invites authorities to apply the technology, even when the regulatory environment may not support it.[25] The reduced need for legislators to practically enable surveillance through legal norms thus affects the impetus for basing such surveillance on clear and foreseeable legal rules. This is exacerbated by the fact that such technologies are more difficult to challenge in court,

16 Lessig (n 14) 126, 129.
17 Hildebrandt (n 1) 121.
18 Hildebrandt (n 1) 124–277.
19 See Nick Fyfe, Helene Oppen Gundhus and Kira Vrist Rønn, *Moral Issues in Intelligence-Led Policing* (2017) 1–20; Nick Tilley, 'Modern Approaches to Policing: Community, Problem-Oriented and Intelligence-Led' in Tim Newburn (ed), *Handbook of Policing* (2nd edn, Willan Publishing, 2008).
20 Though a more manual and resource intensive form of massive surveillance was implemented in many countries during the second world war, in Sweden for example, it has been estimated by the Swedish security service that over 11 million telephone calls were subject to interception during the war years, see Säkerhetspolisen, *Säkerhetspolisens Årsbok 2013* (Swedish Security Service, 2013).
21 See generally Markus Naarttijärvi, *För Din Och Andras Säkerhet – Konstitutionella Proportionalitetskrav Och Säkerhetspolisens Preventiva Tvångsmedel* (Iustus förlag, 2013).
22 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.
23 As it did in the cases from the CJEU invalidating the data retention directive, see Joined Cases C 293/12 and C 594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014], Judgment of the Court (Grand Chamber), 8 April 2014 (ECLI:EU:C:2014:238).
24 See Stephanie K Pell and Christopher Soghoian, 'Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy' (2014) 28 *Harvard Journal of Law & Technology* 1, 9. They described this as "direct and unmediated" surveillance technologies, I use the term direct and discrete here to avoid confusion with the term technologically mediated governing.
25 The Swedish police authority has, incidentally, been using IMSI-catchers since – at least – 2005, without a mandate in law, in violation of EU-law and the European Convention on Human Rights. As the method is secret, the difficulty is however to establish legal standing to challenge this in courts. See Markus Naarttijärvi, 'Swedish Police Implementation of IMSI-Catchers in a European Law Perspective' (2016) 32 *Computer Law & Security Review* 852.

as the details of their implementation and use are known primarily within the agencies using them.[26]

While there has been increased focus on the need for judicial warrants to legally use IMSI-catchers in criminal investigations, the direct and discrete nature of this and similar technologies – like *Finfisher*-like hacking tools – may create a significant delay in the application of judicial controls. Law-enforcement agencies can in effect take advantage of the legal uncertainty surrounding the method, the covert nature of its use, and the direct and discreet nature of the measure to preclude legal challenges. In Canada, law enforcement agencies have been reported to accept plea-deals rather than risk that the use of IMSI-catchers in the investigations become known through discovery and subject to legal challenges.[27] In the United States, secrecy surrounding the same technology has also been attributed to non-disclosure agreements,[28] which brings me to my next point.

2.2 Outsourcing policy choices and acceded secrecy: proprietary private sector product development

A second way in which technology creates obscurity is through what could be described as an 'outsourcing of choice' to the private sector and the associated proprietarisation and confidentiality of policing technology and methods.

In her important work within this area, Elizabeth E. Joh has analysed the 'undue influence of surveillance technology companies on policing' in the United States. She points to how private companies within the surveillance industry make choices in their product development that will influence important aspects of how technology is applied – implicitly affecting policy choices by determining the available choices.[29] This is interconnected with the previously mentioned discrete and direct nature of many technologies, allowing them to function and develop without the law properly mediating between private and public interests. The feature set of such products and their future development may be primarily adapted to larger jurisdictional markets, making the implementation of such products into police forces in jurisdictions for which the product has not been adapted problematic as the product may not fit its particular legal framework. From the point of view of obscurity, a further concern with this proprietarisation is that the features and capabilities of these commercial products may be covered by confidentiality agreements between the producer and the purchasing law enforcement agency, or subject to claims of trade secret protection which may limit the effect of information requests.[30] This may severely interfere with transparency, giving little or no public insight into the actual effects and implications of police powers. It may also hinder legal challenges to their implementation in a certain jurisdiction as police authorities may have agreed to limit the exposure of the technology in court proceedings.

2.3 Changing the equation: the use of existing data in novel ways

A subtler way that technology can mediate the exercise of government power is through emerging ways of analysing and operationalising data already available to law enforcement. Either through new applications of these data, or their use on a scale that was not factored into the original legislative calculation. This is clearly accentuated by the rise of data mining, big data policing, and actuarial justice.[31]

The point here is that technologies like data mining can shift the basic paradigm of policing. Whereas traditional policing is largely incident driven – responding to incoming reports, emergency calls and events,[32] data mining affords law enforcement agencies to adopt more forward-looking approaches where they act on their own initiatives to try to prevent or mitigate future undesirable acts. As Selbst has pointed out, '[d]ata mining allows police to operate unconstrained by theory, finding correlations without worrying why they work'.[33] Causality, in this context, is not as interesting as these correlations, as Joh has noted:

> In criminal investigations, it may not be necessary to know why certain patterns of driving, purchasing, or movement are associated with crime if the police can claim a high correlation between the two. A high degree of correlation itself might provide justification for heightened police attention.[34]

This may also shift the basis for when police powers are used and may circumvent the logic underpinning due process rights surrounding the use of such powers. Traditional concepts such as *reasonable cause* or *reasonable suspicion* regarding individual suspects of a crime that has been committed are difficult to apply in relation to persons finding themselves in an area designated as a potential future crime hotspot, or who have been placed on a 'heat-list' as likely to commit future crimes.[35] Here, the issue is both connected to the translation of risk to traditional evidentiary requirements surrounding coercive powers – i.e. whether a statistical risk is enough to warrant coercive measures – and if the data themselves are trustworthy or carry a potential for hidden biases. However, to a large extent the issue of big data policing relates to the potential for inequitable distribution of police *attention* based on such data.[36] The focusing on police attention is traditionally an issue of police discretion that is largely unregulated, but which carries with it inherent issues of equality and fairness that may be exacerbated by the application of emerging technologies of algorithmic decision-making.[37] Several researchers have pointed to the potential for predictive policing to create feedback loops whereby existing inequalities in the distribution of police attention create a biased data set which focuses even more attention to certain areas or individuals in the future – attention that may not be warranted

26 See section 2.2 below.
27 See in the Canadian context Colin Freeze, 'Guilty Pleas End Risk of Revealing RCMP Surveillance Technology' *The Globe and Mail* (30 March 2016) https://www.theglobeandmail.com/news/national/guilty-pleas-scuttle-hearing-that-risked-revealing-rcmp-surveillance-technology/article29430116/ accessed 11 October 2019.
28 Brad Heath, '200 Imprisoned Based on Illegal Cellphone Tracking, Review Finds' *USA Today* (14 December 2016) https://eu.usatoday.com/story/news/2016/03/31/200-imprisoned-based-illegal-cellphone-tracking-review-finds/82489300/ accessed 11 October 2019.
29 See Joh (n 5) 113–114, discussing police body cameras.
30 See Joh (n 5) 126–126; Selbst (n 1) 189.
31 See Ferguson (n 1); Eubanks (n 1).
32 See Landström et al (n 6).
33 Selbst (n 1) 129.
34 Joh (n 5) 21.
35 Selbst (n 1) 137; Joh (n 5). See also for a more concrete example Vicky Sentas and Camilla Pandolfini, *Policing Young People in NSW: A Study of the Suspect Targeting Management Pan* (Youth Justice Coalition NSW, 2017).
36 Vlad Niculescu-Dincă, 'Towards a Sedimentology of Information Infrastructures: A Geological Approach for Understanding the City' (2018) 31 *Philosophy & Technology* 455, 468.
37 Joh (n 5) 18–19. Niculescu-Dincă (n 36). The inequality of attention may also result in certain victims, not represented in available data, becoming marginalised, see Jonas Lerman, 'Big Data and Its Exclusions' (2013) *Stanford Law Review* [online] https://www.stanfordlawreview.org/online/privacy-and-big-data-big-data-and-its-exclusions/ accessed 1 November 2019.

for the end result of actually preventing crime.[38] Application of data analysis tools may also create what Niculescu-Dincã has described as a sedimentation of design-choices – 'design choices are covered by sediment and thereby invisible, and the prejudices become rock solid in the working routines of the local police. In this way, they can induce a perception of objectivity towards the enacted community, affecting their presumption of innocence'.[39] Another point that has been highlighted by Lyria Bennett Moses and Janet Chan is how algorithmic prediction in policing rests on several assumptions that should be open to challenge, such as the data accurately reflecting reality, that the future will be like the past, and that algorithms are neutral.[40] Some of these assumptions will also negatively affect the transparency and accountability of the process because they are inherent and poorly understood.[41] Given that these assumptions are built into the idea of predictive policing as such, they are sedimented as well, hidden behind software features, and affecting the technological mediation of policing.

The main point here from the point of view of legality is that the application of these new analytic technologies in policing is not necessarily tied to express competences in law, but rather to the changing implication of existing discretionary spaces or areas of legislative inactivity. For example, social media posts are public and consequently law enforcement access to collect and analyse such posts may on the one hand be comparable to observing their surroundings – indeed one might ask: why the police should have less possibilities of observing online discourses than an everyday citizen? On the other hand, law enforcement access to social media posts entails issues that challenge that analogy. Unlike general observations of what happens in the physical world, the police can collect, aggregate, and analyse vast quantities of social media postings in a way which the observation of the physical world does not (yet) allow. As such, social media posts can provide data for analyses of social networks of citizens and afford semantic and mathematical analysis on a vast scale that creates real world implications for the exercise of police powers.[42] Existing commercial software can, for instance, allow police to assign 'threat scores' to persons or addresses in advance of responding to emergency calls, or attempt to identify active gang members. This in turn may change the way police behave and respond to calls, which the police claim can lead to a safer responses to incoming calls, whereas opponents claim the opaque and rough calculus of the software may lead to mistakes which implicitly increases the risk of citizens facing unnecessary force.[43]

38 See Annette Vestby and Jonas Vestby, 'Machine Learning and the Police: Asking the Right Questions' [2019] *Policing: A Journal of Policy and Practice paz035*; Selbst (n 1) 13, 27; Danielle Ensign and others, '*Runaway Feedback Loops in Predictive Policing*' [2017] arXiv:1706.09847 [cs, stat] http://arxiv.org/abs/1706.09847 accessed 14 August 2019; Bernard E Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (University of Chicago Press, 2007) 147–160.

39 Niculescu-Dincã (n 36) 465.

40 Lyria Bennett Moses and Janet Chan, 'Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability' (2018) 28 *Policing and Society* 806, 809–815.

41 Bennett Moses and Chan (n 40) 818.

42 Joh (n 5) 24–26.

43 Selbst (n 1) 137; Joh (n 5) 24–26. See also Brent Skorup, 'Cops Scan Social Media to Help Assess Your "Threat Rating"' (Reuters Blogs, 12 December 2014) http://blogs.reuters.com/great-debate/2014/12/12/police-data-mining-looks-through-social-media-assigns-you-a-threat-level/ accessed 14 August 2019; Justin Jouvenal, 'The New Way Police Are Surveilling You: Calculating Your Threat "Score"' *Washington Post* (10 January 2016) https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html accessed 14 August 2019.

In sum, given that the application of these new technologies may take place without new legislative action, the risks and benefits that they bring may never have been the subject of any democratic deliberation. Yet the practical effects they yield may be substantial – forming the basis for a potentiality of both structural and individualised discrimination, coercive measures, and the translation of risk assessments into practical effects.

2.4 Open code versus algorithmic black boxes

Beyond the impact of emerging technologies on the discretionary spaces of policing powers, their adoption may also obscure the regulation of policing powers as such. If we accept Lessig's idea that code and architecture regulate, he further argues that this type of regulation will affect transparency. It allows the state to hide a regulatory agenda by pursuing it though indirect regulation.[44] As such, it may serve to render regulation – and by extension – the extent of government powers, invisible. Thus, the code that regulates becomes extremely important, and the transparency of that code may be crucial to the maintenance of overall foreseeability and transparency of power. Consequently, Lessig's solution in this regard was the use of open code.[45] Allowing access to the code would help with transparency and open up this type of regulation to scrutiny.

However, since Lessig articulated these arguments, the increased emphasis on 'big data', machine learning algorithms, and AI has highlighted the difficulty of achieving transparency through accessible code. For instance, the logic behind deep learning neural networks is not necessarily comprehensible even for the coders creating them – nor the officers applying them –, awarding them their nickname of 'black boxes'.[46] Indeed, the point of deploying such neural networks is to achieve a better prediction rate in their application than a human could accomplish and regardless of human comprehension of the logic.[47] In this process, the ability of AI or machine learning systems to generate unexpected or 'emergent' results may be regarded by designers as a significant competitive advantage.[48] Certain authors have challenged this idea of obscurity – pointing to the way the design process as a whole can provide some clarity,[49] but the general concern of lacking transparency persists. Furthermore, machine learning algorithms alter their own algorithmic logic in response to new data, continuously developing their prediction model after each new data point.[50] As a result, the underlying code is always evolving, and any transparency of the code will be momentary and fleeting. Finally, and importantly, the ability to predict the effect of a specific algorithm by looking at the code is limited as it will depend on the data it is fed and the quality of those data. Contrary to popular belief, like code – data are rarely neutral, instead they tend to reflect the inherent biases present in whatever environment they originate from. Non-discriminatory code may still produce discriminatory results if the data it is

44 Lessig (n 14) 135-136.

45 Lessig (n 14) 128, 139.

46 See generally Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).

47 Brent Daniel Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 *Big Data & Society* 1, 6; Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 *Big Data & Society* 1, 10.

48 Matthew U Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies' (2016) 29 *Harvard Journal of Law & Technology* 353, 365.

49 Joshua A Kroll, 'The Fallacy of Inscrutability' (2018) 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*.

50 Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 *Big Data & Society* 1, 5.

fed contains a discriminatory bias, either as a result of a biased data source or a non-representative data set.[51]

The response from industry and academia have primarily been centred on countering these problems through the development of AI ethics. While ethical standards relating to AI are important in their own right, ethics is not a panacea. Indeed, the tendency to focus on ethics may risk delaying the activation of democratic structures and the regulation through law, instead relying on soft norms and code to govern the permissible extent of the functions and applications of AI.[52] Going back to the conceptualisation of Kantian ethics, any ethical action must first be legal, indicating a priority of considerations that indicate that ethics should be a complementary, rather than a first order concern in the management of the issues relating to AI.[53] Simultaneously, utilitarian ethics are prevented in many contexts by higher-order legal norms which explicitly express Kantian norms and do not allow for cost-benefit analysis with respect to individual rights.[54]

Consequently, to the extent that an otherwise clear and accessible law facilitates the adoption and use of non-transparent code in decision-making or the exercise of public power, the operation of law will be determined by inaccessible and potentially non-explainable factors – implicitly and indirectly challenging the ability of upholding legality. This brings us to what this concept of legality implies and the extent to which it can tackle the issues highlighted so far.

3. Conceptualising legality

3.1 A theoretical basis for qualitative legality

Legality as a rule of law value is a cornerstone of the modern democratic constitutional order. As an ideal of ruling through and under the law, legality has a long, albeit not straightforward, history in Europe dating back to Ancient Greece and Rome.[55] Today it is well established, at least in a European constitutional context, that the principle of legality may extend beyond a mere requirement that an exercise of government power has a formal basis in law. As will be shown, this wider understanding of legality, which I will refer to as qualitative legality, is influenced by principles of constitutionalism as well as legal theory. It adds several qualitative requirements to the law in question, for instance accessibility, clarity, precision, non-retroactivity, and a general application.[56] The impact of these requirements can be seen most clearly in relation to legal rules which limit fundamental rights where the formal concept of legality is supplemented with a more substantive understanding that focuses on the rule of law qualities of the legal rules. This development has become clearly apparent in the case law of the European Court of Human Rights (ECtHR, or 'the court') in its interpretation of the European Convention on Human Rights (ECHR).[57] Consequently, the same principles are also implicit in the EU Charter of Fundamental Rights.[58] As important rule of law values, they can also be found in the definition of the rule of law articulated by the Council of Europe's Venice Commission.[59]

While subject to development in recent years, qualitative legality is not a new idea as such, nor is it conceptually limited to the context of limitations of rights or within the area of criminal law where matters of legal certainty are most acute. The values implicit in qualitative legality have indeed been expressed more generally within jurisprudence as aspects of an *inner morality of law*, given how they act as internal legal modes of rationality in the absence of which we may question whether a legal system can be seen to exist at all. This understanding has been underpinned by the direct relationship between these qualitative requirements and the ability of law to govern the behaviour of individuals; in the absence of foreseeability, individuals cannot understand what the law requires of them and thus are not able to conform to these requirements.[60]

Most discussions on qualitative legality (or similar concepts by different names) have in common this underpinning of legal authority and legitimacy through the individual's ability to ascertain and understand what is expected of her. As such, legality derives its value largely from the point of view of the individual, where it forms a bastion against unrestricted or arbitrary government power and acting as a precondition for individual freedom and autonomy.[61] In this sense, the qualitative requirements have also been described as something akin to a contractual transaction; if the individual is expected to follow the wishes of the legislator, it is no more than right that the individual can also ascertain what those wishes are and rely on a reasonable interpretation of their legal expression.[62]

51 See Solon Barocas and Andrew Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671; Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1; Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press, 2018); Bennett Moses and Chan (n 40); Selbst (n 1).

52 See Ben Wagner, 'Ethics as an Escape from Regulation. From "Ethics-Washing" to Ethics-Shopping?' in Emre Bayamlıoglu and others (eds), *Being Profiled: Cogitas Ergo Sum – 10 Years of Profiling the European Citizen* (Amsterdam University Press, 2018); Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences.

53 Immanuel Kant, *Grundlegung Zur Metaphysik Der Sitten* (Hoefenberg 2016).

54 For example, the right to human dignity as expressed in art. 1 of the EU Charter of Fundamental Rights, see Catherine Dupré, 'Art 1 – Human Dignity' in Steve Peers (ed), *The EU charter of fundamental rights: a commentary* (Hart [u.a], 2014).

55 Brian Z Tamanaha, *On the Rule of Law: History, Politics, Theory* (Cambridge University Press, 2004) 7-14.

56 See Andrei Marmor, *Law in the Age of Pluralism* (Oxford University Press, 2007) 6–7; Lon L Fuller, *The Morality of Law* (Yale University Press, 1964) 33–95.

57 See Geranne Lautenbach, *The Concept of the Rule of Law and the European Court of Human Rights* (Oxford University Press, 2013); David J Harris, M O'Boyle and Colin Warbrick, *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights* (Oxford University Press, 2014) 506-509; Mattias Derlén, Johan Lindholm and Markus Naarttijärvi, *Konstitutionell Rätt* (Wolters Kluwer Sverige, 2016) 281-284, see further section 4 below.

58 Cf. Sacha Prechal and Steve Peers, 'Article 52 – Scope of the Protected Rights' in Steve Peers and others (eds), *The EU Charter of fundamental rights: a commentary* (Hart Pub Ltd, 2014) 1473. Though the ECJ has yet to put its foot down despite multiple references by advocate generals, the qualitative requirements should at the very least apply in relation to rights corresponding to the ECHR. See also Robert Schütze, *European Constitutional Law* (Cambridge University Press, 2016) 447, suggesting the ECJ applies a material rather than formal concept of law.

59 Venice Commission, *Report on the Rule of Law* (Venice Commission, 2011) 003rev-e, 41 & 44.

60 See Fuller (n 56) 33–95; Marmor (n 56) 6–7.

61 See Tamanaha (n 55) 34-35; Friedrich A von Hayek, *The Constitution of Liberty: The Definitive Edition* (University of Chicago Press, 2011) 320; TRS Allan, 'The Rule of Law' in David Dyzenhaus and Malcolm Thorburn (eds), *Philosophical Foundations of Constitutional Law* (Oxford University Press, 2016) 202, 204; Joseph Raz, *The Authority of Law: Essays on Law and Morality* (Oxford University Press, 2009) 221; also compare Åke Frändberg, *From Rechtsstaat to Universal Law-State: An Essay in Philosophical Jurisprudence* (Springer, 2014) 52-56 who sees them as connected to autonomy and humanism.

62 See David Dyzenhaus, 'Process and Substance as Aspects of the Public Law Form' (2015) 74 *The Cambridge Law Journal* 284, 305; Raz (n 61) 212–223; and in the context of criminal law Petter Asp, Magnus Ulväng and Nils Jareborg, *Kriminalrättens Grunder* (Iustus, 2013) 46.

These understandings of qualitative legality may consequently be described as largely legal-internal in the sense that they revolve around legal/logical arguments such as the ability of law to govern behaviour, internal coherence, or legal certainty. Even to the extent the qualitative requirements have been labelled as 'moral', the morality in question has been described as an inner morality *of law*.[63] Normative legal theories ascribe qualitative legality moral value as it provides law with intrinsic qualities that help explain its authority.[64] In a different vein, opining that the requirements say nothing of the moral character of the aim the law is trying to achieve, but rather how well the law manages to convey and achieve this goal, certain legal positivists have instead described them as functional requirements.[65] In any case, the internal perspective of these theories is to a large extent intentional,[66] and not without merit, as the legal system as such is the object of study and the idea of this system being understood best from the inside has proven capable of generating valuable insights regarding the authority of law.

3.2 Qualitative legality in the practical adjudication of technology: the case of the European Court of Human Rights

The previously mentioned challenges to foreseeability will of course carry with them implications for legality from this internal understanding of the concept. It is, for example, difficult for the individual to ascertain the criteria that will assign her a certain threat score in the algorithmic calculus of police software. Saying nothing about whether this is necessarily the right thing to do, an individual who would prefer to conform to whatever ideal law enforcement would prefer, rather than be deemed a threat, will find that it may be very difficult to do so.[67] This is particularly so if the characteristics adding to a certain score are innate or impossible to alter; such as ethnicity, gender or the socioeconomic status of your parents. It may also be difficult for individuals to assert their due process rights when the use of a surveillance technology is secret or shrouded behind confidentiality agreements.[68] Finally, it is difficult for individuals to challenge privacy violations in courts when the use of a certain technology is known only to the law enforcement agency employing the method and there are no external parties involved.

While these challenges have not always been addressed directly by courts in the context of emerging technologies, there are ways in which qualitative legality can mitigate some of these concerns. To illustrate this, I will use the case law of the ECtHR and its continuous endeavour to uphold the protection of fundamental rights in the face of technological development.

Initially, it is worth noting that the court has held that only publicly available norms can fulfil the requirement of legality (expressed by the court as 'in accordance with the law').[69] Furthermore these norms must reach compatibility with the rule of law – including a certain level of clarity and foreseeability.[70] The application of this foreseeability in a technological context is, however, rather unclear, but it is likely that the ECtHR would approach the issue as one where individual foreseeability of potential consequences is the primary concern – which could imply a requirement of access to internal non-legislative material in order to understand the application of the rules.[71] In contexts such as secret surveillance, where foreseeability cannot reasonably be construed as a possibility for an individual to foresee precisely when the authorities are likely to intercept his or her communication, the concern is instead one of limited discretion of government agencies.[72] In a technological context where there is a potential interference with a convention right such as the right to private life, this will necessitate that government agencies are not given a *carte blanche* to implement any technology they see fit, as doing so would increase discretion to the point of arbitrariness, potentially bypassing existing legal safeguards and failing to meet the standard of legality.[73]

The ECtHR has also been clear that any development in the interpretation of surveillance mandates because of technological development must be foreseeable to individuals through clear and accessible developments in case law. This maintains individual foreseeability when new technology, such as the Global Positioning System (GPS) trackers in the case of *Uzun v. Germany*, are applied, while avoiding legislation that is rigid and unable to handle technological developments that can be contained within a reasonable interpretation of the language of the law.[74] Furthermore, the ECtHR has quite consistently regarded new technologies in light of the safeguards around which their application is surrounded. In the case of GPS trackers, for instance, the court took note of the continuous review by German courts which had the power to disallow evidence.[75] In other cases where safeguards have been lacking, the court has been less inclined to accept surveillance measures.[76]

While cases relating to risk profiling have been rare in the ECtHR jurisprudence so far, the case of *Ivashchenko v. Russia*, regarding the copying of data from a laptop during border controls in Russia, gave the court an opportunity to begin approaching the issue. In this case, the court explicitly dismissed the notion that a risk-profiling approach applied by domestic authorities could be seen as a safeguard against arbitrary interference, when the application of this approach in regards to a specific individual would not be specified.[77] This case may indicate that a wide mandate in law cannot be cured by the application of narrower risk-assessment criteria set out in code. It also indicates that the use of risk-assessment profiles as support for coercive measures will need both a specific and foreseeable legislative basis and explainability in relation to the application of this profile to a certain individual.

63 See Fuller (n 56) 3–91. I will avoid the issue of morality here and use the term qualitative legality as it describes the function of the requirements without having to ascribe nor deny them such moral value.
64 David Dyzenhaus, 'Constitutionalism in an Old Key: Legality and Constituent Power' (2012) 1 *Global Constitutionalism* 229, 233.
65 HLA Hart, Essays in Jurisprudence and Philosophy (Clarendon Press, 1983); Raz (n 61) 226; compare also Marmor (n 56) 35–36.
66 See Dyzenhaus (n 64) 233.
67 Hildebrandt (n 1) 117.
68 See Joh (n 5) 39; Pell and Soghoian (n 24) 34–40.
69 *Leander v. Sweden* (1987) Series A No 116, § 54.
70 See *Huvig v. France* (1990) Series A No 176-B; *Kruslin v. France* (1990) Series A No 176-A.
71 See by analogy *Silver and Others v. the United Kingdom* (1983) Series A No 61, §§ 88-89, which concerned the screening of prisoners' letters, the detailed procedures of which was not set out in law but the prisoners concerned had been made 'sufficiently aware of their content', thereby surviving scrutiny under 'in accordance with the law'.
72 *Malone v. United Kingdom* (1984) Series A No 82. § 68.
73 See *Bykov v. Russia* App no 4378/02 (ECtHR, 10 March 2009) § 77–82, where the Russian legislation at the time allowed law enforcement authorities to conduct 'operative experiments' when investigating serious crime. This allowed unregulated surveillance technologies to be used, bypassing due process safeguards applicable to traditional communications surveillance.
74 See *Uzun v. Germany* ECHR 2010-VI, § 60–74.
75 *Uzun v. Germany* ECHR 2010-VI, § 69–74.
76 See *Ben Faiza v. France* App no 31446/12 (ECtHR, 8 February 2018); Liberty and Others v. the United Kingdom App no 58243/00 (ECtHR, 1 July 2008) § 62; Bykov v. Russia App no 4378/02 (ECtHR, 10 March 2009).
77 See *Ivashchenko v. Russia* App no 61064/10 (ECtHR, 13 February 2018) § 83.

Furthermore, states pioneering the implementation of emerging technologies will be subject to stricter scrutiny. As the court held in *S. and Marper v. the United Kingdom*, a case on the retention of DNA samples in the UK (as opposed to DNA profiles, which is common in other state parties to the convention) of persons no longer suspected or convicted of a crime:

> The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[78]

While this analysis by the ECtHR was made under the umbrella of proportionality, the court noted that the issue of legality in terms of legal safeguards is closely related to the analysis of proportionality.[79] The ruling of the court in the *Marper* case must be tempered by the sensitivity of the type of data involved. However, given the court's tendency to look at the consensus of signatory states to the ECHR when analysing an interference, the implication of claiming a pioneer role in terms of new technologies is likely to be applied in other cases.

This substantive approach to legality in the ECtHR case law has been combined with a dynamic approach to the possibility to lodge a complaint which is of relevance to opaque government measures. The regular approach of the court is to not review convention states' law and practice *in abstracto*, but instead to require individuals to show that they are directly affected by the measure at stake.[80] To allow a legal challenge against secret surveillance measures however, the ECtHR has adopted an increasingly generous approach to legal standing (victim status) under the convention. This was first established quite early on in the case of Klass and others v. Germany from 1978, where the court found that the mere existence of secret surveillance measures combined with the importance of ensuring effective control and supervision of them could warrant exceptions to the main rule.[81] The situations where such an approach could be warranted would, according to the ECtHR, have to be determined on a case-by-case basis.[82] As elaborated in the more recent case of *Kennedy v. United Kingdom*, the principle reason for this departure from its general approach 'was to ensure that the secrecy of such measures did not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and the Court'.[83] This line of reasoning has recently been extensively articulated in the case of *Roman Zakharov v. Russia*. Here, the ECtHR took account first of the scope of the legislation permitting secret surveillance measures and the potential of an applicant being affected by it, and secondly the available remedies on the national level and the effectiveness of those remedies. When there is suspicion and concern among the general public that secret surveillance powers are being abused, those concerns cannot be said to be unjustified in light of weak domestic remedies.[84]

The availability of legal safeguards overlaps with legality not only in the sense that lacking safeguards may result in arbitrary powers as in the cases mentioned above. Giving wide discretionary powers to authorities can result in a situation where individuals face great obstacles in trying to show before national courts that the actions of government authorities have been unlawful or unjustified. The resulting lack of meaningful court review in such cases may in itself create possibilities of abuse or arbitrariness which the court has found problematic.[85]

The approach by the ECtHR in surveillance cases has been interpreted as a sign of the court adopting a republican 'non-domination principle', where the effects of law on the power relationship between the state and citizen are taken into account when analysing the potential violation of a right under the convention.[86] Such an approach could potentially assist the ECtHR in navigating the more abstract and opaque interferences that new technologies such as big data and algorithmic decision-making might cause. A similar rise in non-domination conceptions of privacy and the impact of new technologies has been identified in the case law of the Court of Justice of the European Union (CJEU), where it has been linked to the need to restrict the accumulation of arbitrary powers.[87]

These developments in the case law of the ECtHR and the CJEU, while far from offering a comprehensive approach to new technologies, may help maintain legality in the sense of individual foreseeability. It provides a minimum level of transparency and foreseeability of government measures that may be applied to technologically mediated government and could help individuals challenge certain opaque measures. However, in approaching these issues, it is important not to lose track of the role that qualitative legality plays in a larger constitutional framework – extending beyond the individual to the democratic core of the state. This role will be further analysed in the following section and it will eventually give us a reason to return to, and elaborate on, the principles drawn up by the ECtHR.

4. Legality and democracy: dusting off Implicit interconnections

The theoretical outline I have previously presented of the concept of qualitative legality has largely been focused on legal certainty and foreseeability for individuals and the preservation of internal legal rationality. However, the maintenance of foreseeable legislation in the face of technologically mediated governing also carries with it important implications for democracy which will here be analysed further.

Assuming we base our understanding of legal legitimacy on the fulfilment of rule of law ideals, it follows from the implications to foreseeability that technologically mediated governing risks undermining the

78 *S. and Marper v. the United Kingdom* ECHR [GC], 2008-V, § 112. See also *Aycaguer v. France* App no 8806/12 (ECtHR 22 June 2017).
79 *S. and Marper v. the United Kingdom* ECHR [GC], 2008-V, § 98.
80 See *N.C. v. Italy* ECHR [GC] 2002X, § 56,; *Krone Verlag GmbH & Co. KG v. Austria* (no. 4) App no 72331/01 (ECHR, 9 November 2006) § 26; *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* ECHR [GC] 2014-V, § 101.
81 *Klass and others v. Germany* (1978) Series A No 28, § 34.
82 *Klass and others v. Germany* (1978) Series A No 28, § 34.
83 *Kennedy v. the United Kingdom* App no 26839/05) (ECtHR 18 May 2010) § 124.
84 *Roman Zakharov v. Russia* ECHR [GC], 2015-VIII, § 171.
85 *Ivashchenko v. Russia* App no 61064/10 (ECtHR, 13 February 2018) §§ 88-92.
86 Bart van der Sloot, 'A New Approach to the Right to Privacy, or How the European Court of Human Rights Embraced the Non-Domination Principle' (2018) 34 *Computer Law & Security Review* 539.
87 See Andrew Roberts, 'Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications: Privacy, Data Retention and Domination' (2015) 78 *The Modern Law Review* 535.

legitimacy of legal rules. This intra-legal legitimacy is however implicitly tied to broader issues of democratic legitimacy. The foundation of this democratic legitimacy can be sought in different sources. I will proceed with a conceptualisation of *democratic* legitimacy inspired by consent theories and the theory of deliberative democracy articulated by Jürgen Habermas. While I acknowledge that this is a concept that carries with it a somewhat thicker understanding of the 'oughts' of democratic processes, I believe it is one that resonates with most European democracies as a hybrid of liberal and republican values.[88] The implications I point to will in any case prove relevant in constitutional contexts where parliament carries the core of the democratic grounding of state power and where the separation of power is functionally important.

4.1 Qualitative legality as catalyst of deliberation

The idea of parliament as a democratic shorthand for 'the will of the people' is based on a presumption of the democratic nature of parliamentary law making. This democratic nature has its basis in both the direct nature of parliamentary elections, and in parliament as a place for democratic discourse and debate.[89] In its ideal form, the legislative process will subject bills to scrutiny and deliberation, and through this process parliament will both increase the quality of the bill through rational argumentation and ensure that their content can gain a majority support by the representatives of the public.[90] While doing so, the elected will be subject to pressure from the public and interest organisations, and to scrutiny by the media, ideally fulfilling the role of bringing issues from the periphery into the centre of public and political discourse. Meanwhile, on a political level, parliamentarians are subject to pressure from their party, the executive branch, and their primary constituents.[91] As emphasised by Habermas, the resulting discourse is the foundation of democratic legitimacy. It also implies something else. By ensuring that law is the result of a transparent democratic discourse, citizens – ideally – can see themselves as co-authors of the law they are subject to.[92]

Qualitative legality, as discussed above, can strengthen this democratic deliberation in several ways. By converting the political goals of the elected into legal norms, public policy is given a shape that allows legal-internal rationality and rule of law values to be upheld and makes politics legally enforceable.[93] As pointed out by Dyzenhaus, law's claim of authority must be understood as an implicit claim of legitimate authority, where legitimacy is dependent on legality as a rule of law value, creating the preconditions for a genuine social contract and consent, and where the subjects of the law are autonomous and partners in the rule of law project.[94] Qualitative legality thus ensures a connection between the law and the interests of the people as expressed through the elected legislative assembly's political deliberations and decisions. Indeed, the clearer the connection is between the actions of the state and the concrete legal form of the political decisions resulting from the deliberative and reflective process of representative democracy, the more democratic legitimacy. Maintaining qualitative requirements of legality will uphold a vital link between the language of the law (which holds democratic legitimacy through the deliberations and decisions that precede it) and the actions and decisions of the state.

The logic behind this argument becomes clearer if we think about foreseeability as something having effects in two directions. On the one hand, the individual is supposed to be able to foresee the effects of law on her actions, but this is practically impossible if legislators are not able to foresee the effects of law as mediated through technology. As these practices drift from what the legislator explicitly or implicitly could have foreseen, the legislation loses connection with the deliberative processes of democracy that underpin its legitimacy.[95]

The need to reach qualitative legality requirements further serves to create and increase transparency, enabling the democratic discourse surrounding current or proposed laws to be based on reasonable levels of foreseeability regarding the potential effects of those laws in relation to, for example, the impact on constitutional rights. Conversely, deficiencies in qualitative legality may result in a situation where neither citizens nor elected legislators really understand the implications of a proposed law, nor the power it confers to the executive. This is especially important when the legal practice is opaque or secret. One poignant example of this can be found in the United States where neither legislators nor citizens seemed able to foresee the vast surveillance system enabled by a vague section of the *USA Patriot Act* and the powers the executive government would eventually carve out of it.[96] While the (unintended) visibility of these surveillance practices through the disclosures of Edward Snowden did not lead to their discontinuation, it did contribute to the democratic debate on the security services' methods being based on a higher degree of foreseeability into the actual effects of the legislative framework and the actions of government agencies.[97] It has also allowed citizens to show standing to challenge the legality of the surveillance regime and the participation of their governments in it.[98]

In this context, qualitative legality serves an additional important function. It serves to uphold the separation of powers by limiting the discretionary power of the executive, while also upholding legal certainty by requiring that individuals can foresee what law requires and the authority given over them to executive agencies. This is mirrored in that clarity with regards to effects and powers conferred enables the elected representatives to foresee the scope of the power

88 For this interpretation of Habermas, see Lasse Thomassen, *Habermas: A Guide for the Perplexed* (Continuum, 2010) 121.

89 This idea recently received normative force in the German Federal Constitutional Court's decision on the European Financial Stability Facility and the ESM/Euro Plus Pact, where the court held that the Bundestag's right to decide the budget have to be exercised through deliberation and decision-making in the plenary setting rather than delegated to a committee or to the executive or a supranational mechanism, see Tony Prosser, 'Constitutions as Communication' (2017) 15 *International Journal of Constitutional Law* 1039, 1061.

90 See Jürgen Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (Polity, 1996) 304–306.

91 Antje von Ungern-Sternberg, 'German Federal Constitutional Court Parliaments — Fig Leaf or Heartbeat of Democracy? Judgment of 7 September 2011, Euro Rescue Package' (2012) 8 *European Constitutional Law Review* 304, 320-321; See also Prosser (n 89) 1059–1061.

92 Habermas (n 90) 449.

93 Dyzenhaus (n 62) 297.

94 Dyzenhaus (n 64) 259.

95 Cf. Habermas (n 90) 450; see also Tamanaha (n 55) 99-100. In the same vein, the connection to the proportionality assessments made by the legislator becomes less pronounced as well, indicating the need for a stricter review by courts. This is however a matter for a different discussion.

96 See Jim Sensenbrenner, 'This Abuse of the Patriot Act Must End | Jim Sensenbrenner' *The Guardian* (9 June 2013) https://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end accessed 14 August 2019.

97 Illustrative in this context are the investigations by the German Bundestag – the 'Untersuchungausschuss "NSA"' – and the EU parliament investigations 'The US surveillance programmes and their impact on EU citizens' fundamental rights' (PE 474.405) and 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI)).

98 See *Big Brother Watch and others v. the United Kingdom* App no 58170/13 (ECtHR, 13 September 2018).

handed to the executive and enables an informed democratic debate and discussion on such transferals of power based on a reasonably foreseeable practice.

While qualitative legality can fulfil these democratic functions, it is challenged when the actual effect of law is mediated through technology in ways that impacts foreseeability. In such cases, democratic discourse might be based on limited information and with a diffuse conception of the actual implications of laws under deliberation. It may result in a situation where legislators cannot reasonably foresee the implications of a law or the powers it confers to the executive government, either through a wide interpretive space, or through technological developments that carve out further power from discretionary spaces over time. It may also allow governments to hide or disguise the exercise of power, by clouding them in code. As Lessig puts it, '[c]ode-based regulation – especially of people who are not themselves technically expert – risks making regulation invisible.'[99] He argues that transparency serves as an important check on government power and the only rules government power should impose are those that would be obeyed if imposed transparently.[100]

In the context of technology, these transparent deliberative practices are sometimes described as difficult to achieve due to a perceived inability of the public to navigate complex technological issues that arise in many policy areas. This has led to a questioning of the ideal of deliberative democracy in this context.[101] More recent research in science and technology studies (STS) has however challenged this assumed ignorance and explored instead the differing points of departure from which people navigate and question technological choices and social dilemmas. These viewpoints and experiences may be different from those of experts and politicians, but equally valid and complementary, highlighting the need to maintain public deliberation of emerging technologies and their implications.[102] In any case, it is fairly obvious that navigating complex social and technological issues is not made easier by keeping them opaque and vague. In fact, a more transparent democratic deliberation can assist governments in achieving compliance with human rights norms, avoiding issues with both legality and proportionality.[103]

An example from Sweden illustrates this. In 2007 a government bill intended to give the Swedish signals intelligence agency (FRA) access to all wired network traffic crossing Swedish borders to allow for automated searches for combinations of keywords and characteristics deemed relevant for national security, so called 'massive interception' or 'bulk collection'.[104] This led to significant public debate and parliamentary infighting, even within the ruling coalition government, over fears of mass surveillance. To pass the bill, the government announced proposals to strengthen the oversight mechanisms, adding – among other things – a court review of search terms and limiting access to only those fibre optic information carriers which are likely to be relevant for the particular intelligence target.[105] These changes were recently highlighted by a chamber judgment of the ECtHR as key aspects making the law acceptable under the ECHR.[106]

Consequently, the public and parliamentary debate did not only force the government to increase oversight, it also forced it to articulate rather vague and potentially wide legislative language into something more specific and transparent that ultimately managed to gain support in parliament and which may yet survive scrutiny by the ECtHR.[107] This, in turn, served to limit the discretionary space of the signals intelligence agency, maintaining a minimum level of legality, while simultaneously calming the concerns from parliamentarians and certain sections of the public.

This ability of deliberative practices to 'act as a prophylactic against later costly lawsuits'[108] is often forgotten. In a constitutional context it can also reduce the risk of legal uncertainties because of legislation that is expensive to implement, yet cannot for long be applied or is simply declared invalid following a decision by a court.[109]

4.2 Allowing autonomy and fostering cross institutional discourse

So far, I have touched upon the role qualitative legality plays for the legislative process. There are, however, further functions that qualitative legality can fulfil to allow for a broader deliberative discourse in a democratic state.

As mentioned above, democracy is more than a simple expression of popular will, it is grounded in a *process*. As conceptualised by Habermas through his co-originality thesis, any democratic system must capture both public and private autonomy, ensuring that citizens have a standing to both express a political will and assert their constitutional rights.[110] In this process, courts are tasked with the important role of interpreting and applying law as well as acting as guardians of individual rights. As the ECtHR has concluded, a gradual and foreseeable development of law through legal precedent is not incompatible with qualitative legality.[111] As far as interpretation of legislative acts goes, there is a point however, where the connecting strands between a legally authoritative interpretation which is foreseeable due to gradual developments in case law, on the one hand, and the democratic legitimacy of parliament on the other, is severed. The question then becomes if the legal system can cure a lacking *ex ante* democratic deliberation regarding a specific technological reality with *ex post* judicial means of maintaining individual autonomy? If we adopt a wider understanding of how and when the deliberative practices can be realised, we can reasonably include not only the ability of citizens to engage in public discourse in advance of legislative measures being put in place, but also the way citizens may challenge the constitutionality of law and government measures in courts, asserting their autonomy as legal subjects and actors within a constitutional framework. In doing so, they can bring constitutional issues under the purview

99 Lessig (n 14) 138.
100 Lessig (n 14) 328.
101 See Patrick W Hamlett, 'Technology Theory and Deliberative Democracy' (2003) 28 *Science, Technology, & Human Values* 112, p. 125.
102 See Peter Newell, 'Democratising Biotechnology? Deliberation, Participation and Social Regulation in a Neo-Liberal World' (2010) 36 *Review of International Studies* 471, 477–478, discussing the context of environmental risk and GMO.
103 Hamlett (n 101) 130.
104 Swedish Government Bill [2006/07:63].
105 Swedish Government Bill [2008/09:201].
106 See *Centrum för Rättvisa v. Sweden* App no 35252/08 (ECtHR, 19 June 2018) § 180.
107 The case has recently been referred to the Grand Chamber of the ECtHR.
108 Hamlett (n 101) 130.
109 The invalidation of the EU data retention directive and the subsequent rejection of its national implementation law in Sweden is a poignant reminder of this, see Joint cases C-293/12 & C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others, and Kärntner Landesregierung and others*, EU:C:2014:238; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (2016), Judgment of the Court (Grand Chamber) of 21 December 2016, ECLI:EU:C:2016:970.
110 Habermas (n 90) 121–123.
111 See section 3.2 above.

of courts – essentially activating a constitutional discourse between courts, government, and parliament.[112]

This control will in turn enable the autonomy and dignity of the individual to be safeguarded, and as such the preconditions for both the formation of public opinion, the expression of this opinion, and the retention of a democratic system that allows individuals to authorise future legislative assemblies to act on their behalf.[113] To enable this, courts must however be open to a more generous approach to standing, as the sometimes subtle *individual* effects can mask more overarching *systemic* issues. In this sense, the ECtHR with its dynamic approach to victim status in surveillance cases can be one example of how to balance the interests involved.[114]

I believe this perspective is a fruitful addition to the concept of republican non-domination as it is connected to similar ideas – distribution of power, our relationship as citizens with government bureaucracies, and the avoidance of discretionary power.[115] It also engages similar issues of democratic inclusion as a counteraction to domination.[116] But it also engages with further questions of power transferrals between government branches, the existence of deliberation regarding the application of a specific technology, as well as the possibility for individuals to assert themselves as autonomous legal actors through the courts.

This brings us to the question of how legality may be understood to safeguard both individual and democratic functions in the light of technologically mediated governing and black box policing. Or, in other words, how should legality be recoded to fit within a technological legal framework?

5. Qualitative legality recoded

The central issue that this contribution has so far orbited (albeit in a rather twisted trajectory) is how technologically mediated governing – particularly in the policing context – can be legally contained and regulated, and how legality in the context of such governing can be upheld in adjudication. So far, I have primarily focused on certain challenges relating to technologically mediated governing and pointed to some tentative responses to those challenges from the ECtHR. I have also outlined the legal and democratic functions that legality fulfils and in doing so attempted to highlight the values that regulation and adjudication in this context should try to uphold. In the following, a more constructive approach, with every intellectual peril that entails, will be attempted.

5.1 Technology neutrality

While academics have, as is evident above, pointed to the risks involved in allowing new technologies to run rampant through the regulatory environment of policing, the response from legislators has often been considerably more innovation-friendly. This is especially evident through the concept of technology neutrality that has been a staple of technological regulation in both the EU and the US since the 1990s.[117] As put by Reed, the idea that law should not pinpoint a certain technology, but rather keep itself open to technological development by remaining technology neutral, has been regarded as naturally good, 'like motherhood and apple pie'.[118] This ideal, however, is likely to exacerbate the very issues highlighted here. The point of technology neutral law is often to allow authorities to choose suitable technologies to achieve a government policy, thereby avoiding rigid or outdated legislation. To achieve this, purposes or generalised technological concepts are described to avoid specific references to technology which may become outdated. However, qualitative legality as a concept would (anthropomorphically) frown upon precisely this form of discretion. Not only does it create uncertainty as to how the law is to be interpreted in relation to emerging technology, but the technological affordances that were the point of departure for the deliberations in the legislature may fundamentally shift. The gradual adaptation to new technology that technology neutrality was supposed to ensure, may instead create wide discretionary areas of technologically mediated governing. The risk, essentially, is a transferral of power from parliament (choosing to open up the discretionary technological space) to the executive agencies implementing a certain technology which, depending on the context, may never be subject to review by a court. The black box of policing discussed above is, in other words, nourished by the apple pie of technological neutrality.

In this context, it is worth keeping in mind that there are two distinct types of neutrality. First, there is a very reasonable ideal that constitutional rules and principles should be insusceptible to technological change. As Lessig puts it, judges are translators:

> We must always adopt readings of the Constitution that preserve its original values. When dealing with cyberspace, judges are to be translators: Different technologies are the different languages, and the aim is to find a reading of the Constitution that preserves its meaning from one world's technology to another.[119]

In terms of the second type of neutrality, which provides government agencies with mandates to exercise power through legislation that does not specify technological means, there is however a risk that technology neutral legislation instead codifies a form of indifference to the importance of code and architecture. It becomes in effect a transferal of power from the democratic arena to the architects of the digital arena; in some cases, this shifts power from the state to markets, in others from parliament to government agencies. In many cases it is both.

It is worth considering that the requirements of qualitative legality, including the deliberative aspects I have argued for above, may demand a more specific legislation – at least in such legislative contexts that may affect individual rights or the power relationship between citizen and state. The need to revisit legislation more frequently in view of new technological developments, while understandably a complicated and time-consuming process, may be a worthwhile price to pay to foster both legality and democratic legitimacy in the technological context.

5.2 A more extensive interpretation of legality

To counter unconstrained transferrals of power, we need to understand the implications of technology, not just in terms of certain individuals or groups at risk of suffering adverse effects, but also the shifts in the power relationship between individuals and the govern-

112 Prosser (n 89) 1059–1061.
113 Cf. Mattias Kumm, 'Democracy Is Not Enough: Rights, Proportionality and the Point of Judicial Review' (Social Science Research Network 2009) SSRN Scholarly Paper ID 1356793 https://papers.ssrn.com/abstract=1356793 accessed 14 August 2019.
114 See section 3.2 above.
115 See Andrew Roberts, 'Forewords · Why Privacy and Domination?' (2018) 4 *European Data Protection Law Review* 5.
116 Ludvig Beckman and Jonas Hultin Rosenberg, 'Freedom as Non-Domination and Democratic Inclusion' (2018) 24 *Res Publica* 181.
117 See generally Chris Reed, 'Taking Sides on Technology Neutrality' (2007) 4 *Script-ed* 263; Paul Ohm, 'The Argument against Technology-Neutral Surveillance Laws' (2010) 88 *Texas Law Review* 1685.
118 Reed (n 117) 264-265.
119 Lessig (n 14) 165-166.

ment. Conceptualising the legality of new technologies must therefore go beyond 'due process legality', focusing on the particular effects of an individual, and *also* ask wider questions regarding the transferral of power from law – the purvey of parliament – to the technologically mediated bureaucracies of executive agencies and the private technology companies they rely on.

As courts analyse the legality of a certain measure, they should consider the potentialities of technology to shift power relationships within the branches of government and between state and private actors. In doing so, even within the limits of a single case, courts may need to consider the wider implications of a certain technology and whether they are transparent and foreseeable not only for the individual, but also whether they were ever the subject of democratic deliberation at all.

Admittedly, extending the analysis of legality beyond the case at hand might extend the purview of the court into what some may believe would amount to judicial activism, and the counterargument may be that courts should instead defer to the government if in doubt. I would however argue that when the legislator has not even considered the use of a certain technology, there is no legislative will of parliament to defer to.[120] Deferring to the government in such cases would instead cause an implicit transferral of power from parliament to the executive that was never intended. In contrast, by keeping in mind the democratic functions of qualitative legality and strictly analysing the legality of a technological measure in that light, courts instead serve parliamentary supremacy by essentially turning the question back to the proper place for democratic deliberation. In doing so, courts will essentially say; 'if this is what parliament desires, it will at least have say so explicitly, transparently, and after deliberating on the issue'.[121]

5.3 Judicial pre-review and extensive *ex post* review

One way in which the application of new technologies could be better insured against a departure from the requirements of legality, while maintaining some flexibility, is through preliminary court reviews of new technologies being implemented within public agencies that may affect individual rights or due process.

While such reviews of legality are often conducted within executive agencies prior to the application of certain methods or technologies, the addition of a court review could fulfil functions that improve qualitative legality in several ways. Following an internal review of the legislative framework surrounding a new or previously untested method, a law enforcement agency could apply to a court to get a preliminary approval of its use, making their best arguments for why it may be legal. This hypothetical court review could then consider both how well the new technology fulfils existing requirements of legality and proportionality, as well as its fit within legal mandates and due process requirements. Simultaneously, civil society organisations, bar associations, and other stakeholders could file their own briefs to inform the court. Should the method not fit within the existing legal and deliberative framework (i.e. considering the degree to which the method could have been foreseen and deliberated within the democratic process), the court could refer the issue to the legislature. Should it fit, but with certain caveats, the court could put in place such terms and conditions that are required to limit the use of the technology to what is allowed within the framework of constitutional or human rights rules. Such a preliminary review could also make relevant legal aspects of the application of the method public, reaching the transparency and foreseeability requirements similar to the case of *Uzun v. Germany* mentioned in section 3.2 above.

The use of preliminary review of specific technologies is different from other measures such as judicial review *in abstracto*, as it focuses not on the legal rules themselves, but instead on the technologies used and how they fit within a legal framework. Comparable solutions implemented within a political framework exist in certain US cities, most famously in Seattle, where a city surveillance ordinance requires the police to report the use of surveillance technologies onto a 'master list' which is then subject to public deliberation and city council review. It is intended to increase political control of surveillance technologies and to increase civil society involvement while increasing public trust in the police.[122] While the Seattle ordinance has been seen to not properly address the use of algorithmic surveillance,[123] it is still a noteworthy example of how technologies can be subjected to increased scrutiny.

While the publication of details of surveillance methods is – to put it mildly – frowned upon by intelligence and law enforcement agencies, the clarification of more general attributes of surveillance mandates (such as the general scope of its intrusion into a right and the safeguards surrounding it) and the relevant legal aspects of how a technology can be reconciled under a legal mandate, are in any case of the type that needs to be publicly available to reach legality requirements (as they are construed by the ECtHR).

To avoid the negative effects of technology neutrality discussed above, a pre-review should strive to delineate the salient features and underlying presumptions that distinguish the legal analysis of the method in terms of impact on individual rights, principles, or rules. This will ensure that shifts in technologies impacting those underlying features and assumptions will necessitate a new review. In relation to surveillance technologies, this could imply a description of the limits in terms of the degree to which the method allows for the mapping of individuals or groups. In relation to the implementation of machine-learning algorithms, this could imply a description of the necessary level of human involvement in decision-making, restrictions on allowed applications, attributes or inferences, restrictions in the further measures taken based on automated profiles, necessary measures to quality assure underlying data sets, or safeguards in terms of *ex post* auditing.

It is important to note that a review, such as the one outlined above, can only ever be preliminary and must not be allowed to prevent a later *ex post* judicial review of the application of the technology used. As discussed in previous sections, the actual effects of a certain technology are in many ways dependent on its application and its interface with citizens. The preliminary review can, however, ensure a legal check on otherwise discrete and direct technological measures. It would also serve as a continuously updated inventory of techno-

120 This conclusion is inspired by that of the ECtHR judge Robert Spano, opining that deference to national parliaments in questions of proportionality is not a valid argument in the cases where the national parliament has never considered the proportionality in the first place. Robert Spano, 'The European Court of Human Rights and National Courts: A Constructive Conversation or a Dialogue of Disrespect?' (2015) 33 *Nordic Journal of Human Rights* 1, 7.

121 See further Markus Naarttijärvi, 'Kvalitativ Legalitet: Ett Demokratiskt Perspektiv' (2018) 131 *Tidsskrift for Rettsvitenskap* 206, 206-234.

122 See Meg Young, Michael Katell and PM Krafft, 'Municipal Surveillance Regulation and Algorithmic Accountability' (2019) 6 *Big Data & Society* 205395171986849. Similar ordinances exist in Berkeley, Cambridge, Davis, Nashville, and Oakland.

123 Young et al (n 122) 12.

logical methods and measures developed or applied within government agencies, increasing transparency. Even if certain aspects or methods would need to be kept under a shroud of secrecy, access to these decisions by oversight organs, researchers, and parliamentary committees would inform the legislative process in the technological context.

5.4 *Ex post* auditing

The importance of algorithms and the data that fuel them is becoming increasingly clear, and there have been increased efforts to ensure some insight into algorithms. In Europe, this push has not been fuelled by concerns of legality, but rather from the viewpoint of data protection, privacy, and informational self-determination. Within the European Union, steps have been taken to try to achieve transparency and limit the impact of profiling and algorithmic decision-making through legislation such as the new EU General Data Protection Regulation (GDPR).[124] Article 13.2(f) GDPR specifically requires the provision of meaningful information about the logic involved in automated decision-making and profiling, as well as the significance and the envisaged consequences of such processing of personal data for the data subject. There is a further rule in article 22, giving data subjects a right not to be subject to decisions made *solely* on automated processing, including profiling, which produces legal effects for him or her or significantly affects him or her. However, the impact of this rule is limited in two primary ways. First, the rule only applies to *fully* automated decision-making – including a human in some part of the decision-making process will circumvent the rule as long as the human has meaningful impact on the outcome.[125] Second, the GDPR does not apply to processing of personal data within law enforcement and while there is a similar rule in the directive harmonising data protection in that context, it is possible for member states to allow such automated decision-making through national law though not based on certain sensitive categories of data.[126]

Still, the impulse to ensure access to and information about algorithmic decisions based on citizen data is reasonable. Even when the applications of technology are in accordance with the law, transparency can create awareness of how data are used and how government agencies (and, in the case of the GDPR – even private actors) reach their conclusions based on these data. It is however difficult to achieve full transparency, both on account of the technologies involved such as neural networks where the logic may make review fruitless, and because true understanding of the outcomes will require access to the underlying data, which may end up conflicting with privacy and data protection of others whose data are being processed. There may therefore be an increased need for expert auditing of big data governing from oversight bodies where access to information and technological experts can be achieved more effectively.[127] Importantly, the organs auditing such technology should be given mandates which are not tied to express technologies or policing powers as this runs the risk of new technologies being implemented in the gaps between these mandates. Instead, their auditing mandates should be wide and overarching to allow their audit to adapt to changing circumstances.

5.5 Avoiding determinism

The advent of technologically mediated governing does not entail a necessary surrender of legal values to the unrelenting march of technological development. Technology challenges the existing framework of legal governance and involves inevitable difficulties in regulating technology. However, as noted in STS literature, the surrender to technological determinism through the idea that technological change causes or determines social change 'leaves no space for human choice or intervention and, moreover, absolves us from responsibility for the technologies we make and use'.[128] In fact, there is nothing forcing government agencies to employ technological measures or make governing dependent on their application. Indeed, while technological determinism is often visible in the debates on regulating social media, drones, or AI for private entities, the normative influence of law within government entities is, or at least should be, higher. As such, even while we may accept the difficulty of effectively preventing a certain technology from affecting the everyday life-world of private citizens or private entities, this does not answer the question of whether we should allow or pursue the use of the same technology within our government agencies. Instead, these are choices governments can make and abandoning these choices to the whims of technological trends will fundamentally weaken the sphere of democratic deliberation. As Lessig puts it: 'Code codifies values, and yet, oddly, most people speak as if code were just a question of engineering. Or as if code is best left to the market. Or best left unaddressed by government.'[129]

Avoiding this determinism requires us to 'recode' legality to fit a technological context. Doing so will essentially require three main considerations to be actively acknowledged in both the legislative process and the adjudication of technologically mediated governing.

First, as I have pointed out above, the legislative process must be based on a reasonable level of foreseeability regarding the interaction between law and technology. This may require the abandonment of technology neutrality as a legislative ideal in contexts where technology will interfere with rights, alters the power relationship between citizen and state, or when it significantly affects the balance of power within a constitutional system. If government power should be bound by law, technology cannot be exempt from this.

Second, the review of legality of technological measures by courts should consider the existence of deliberative practices underpinning

124 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).

125 As put by the Article 29 Working Party: 'The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data.' See Article 29 Working Party, '*Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*' (Article 29 Working Party 2018) wp251rev.01, 21.

126 Article 11, Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

127 See Paul B de Laat, 'Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?' (2018) 31 *Philosophy & Technology* 525.

128 Sally Wyatt, 'Technological Determinism Is Dead; Long Live Technological Determinism' in Edward J Hackett and others (eds), *The Handbook of Science and Technology Studies* (3rd edn, MIT Press, 2008) 169.

129 Lessig (n 14) 78.

the measure under review. While a certain technology may fit into the semantic meaning of a legal provision, the effects produced may never have been possible for legislators to envision. While the point here is not that every consequence of technology must have been foreseen – which would make law unbearably complex and rigid – measures that will substantially impact rights or the power relationship between citizen and state, or parliament and the executive, should be subject to a stricter review.

Third and finally, the many subtle ways in which technologically mediated governing can influence individuals will require courts to have a dynamic and generous approach to standing. Here, the approach taken by the ECtHR can serve as inspiration. I have also suggested the implementation of a form of preliminary judicial review of new technologies that could assist in the fulfilment of qualitative legality in the application of emerging technologies in governing. In combination with a strict ex post court review and auditing by expert oversight bodies with access to both code and data, this could aid in the mitigation of the concerns raised here.

5.6 The choices we make

As we have seen, there are several important implications of technologically mediated governing for both legality as a rule of law value, and the implicit democratic values legality serves. This is true both in the context of policing and in other fields of governing. The pertinent question raised is whether automation of government decision-making will itself shape the rule of law.[130] If the development of the rule of law has made the exercise of government power subject to the law, increased foreseeability, and limited arbitrariness, we may indeed reasonably ask whether technologically mediated governing will move important aspects of this governing into a black box. In this box, the norms that govern are statistical rather than legal. The goal of foreseeability is replaced by ambitions of accuracy, and if human discretion is replaced, there is an inherent risk that it is replaced by an automated naivety regarding the systematic inequality which is represented in the data that surround us. Avoiding this will require us to interpret legality in a way that maintains both the explicit and implicit values it protects even in the face of technological change.

Acknowledgements

The author would like to thank the arrangers and participants of the *TILTing* 2019 conference, as well as the editors and anonymous reviewers of Technology and Regulation for valuable comments that helped inform and improve this paper. This contribution is a result of the project 'Policing in Sweden – Efficiency and Rule of Law in Police Work', the funding for which has generously been provided by Riksbankens Jubileumsfond (The Swedish Foundation for Humanities and Social Sciences), grant no. SGO14-1173:1. Parts of chapter 3 and 4 are built upon ideas the author has previously discussed in Swedish in Tidsskrift for Rettsvitenskap, vol. 131, 2–3/2018 p. 206–234, available at: https://www.idunn.no/tfr/2018/02-03/kvalitativ_legalitet

130 Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'The Rule of Law and Automation of Government Decision-Making' (2019) 82 *The Modern Law Review* 425. See also Emre Bayamlıoglu and Ronald Leenes, 'The "Rule of Law" Implications of Data-Driven Decision-Making: A Techno-Regulatory Perspective' (2018) 10 *Law, Innovation and Technology* 295, 311.