Editorial

The right to privacy, like other fundamental rights, initially applied to vertical relations. It curbs the state's monopoly on power by setting rules and limits for government interference in the private lives of citizens, such as through entering homes, collecting personal data, monitoring correspondence and carrying out bodily searches. Since the first years of this century, with the rise of tech giants such as Google, Facebook, Microsoft and Apple, there has been increasing attention for so-called diagonal privacy. Although these companies do not have a monopoly on power, their resources and capacities for engaging in privacy interferences are perhaps even greater than those of government agencies, not in the least because these companies, often based in the United States, are bound by fewer rules and restrictions. Recently, so-called horizontal privacy has gained renewed momentum. The background to this is the fact that citizens have easy access to all kinds of technologies and products with which they can violate each other's privacy.

One problem, however, remains largely unaddressed for the time being: what if Little Brother turns against Big Brother? What if citizens turn their power against the state? Fundamental rights are traditionally seen as protecting citizens from the state, but how tenable is this doctrine when the state, public office holders and government officials are themselves increasingly the victims of citizens' use of power? Is Big Brother still the all-powerful party against whom the citizen must be protected, or should the combined power of the millions of Little Brothers now also be a fear of the government? Should we introduce a new concept, something like ‘reversed vertical privacy’?

Current legal doctrine is in many respects still grounded in traditional conceptions: the state has a monopoly of power, the government and politicians, because they have power, have additional transparency obligations and should endure more scrutiny from the public eye and the state and its civil servants should be neutral. For example, Article 11 of the European Convention on Human Rights (ECHR), which enshrines the right to assembly and association, provides that states may impose restrictions on the exercise of those rights by public servants. ‘This article shall not prohibit the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.’ Such provisions are intended to ensure the neutrality of the state. Civil servants must disregard their personal views, philosophies and political opinions when performing their duties, something that can also be seen in the uniform requirement for police and other services and the ban on wearing religious symbols in many European countries.

For politicians, it is the other way around, they have wider freedoms when it comes to taking up positions in the public debate and can count on fewer limits than ordinary

DOI: 10.21552/edpl/2021/2/3

citizens when it comes to expressing extreme, controversial or dubious views. The other side of this coin, however, is that they have to reckon with extra scrutiny and attention from the public and the media. Although the European Court of Human Rights is of the opinion that politicians must also be able to count on protection of their privacy, even in the public space, it has also emphasised that public figures must endure additional scrutiny, that far-reaching investigations in their private sphere and publication about private matters are permissible, and that they can also count on less protection when it comes to their right to reputation, as contained in the right to privacy, Article 8 of the ECHR. 'Not only do the media have the task of imparting such information and ideas; the public also has a right to receive them. This is all the more so where public figures are involved, such as, in the present case, the applicant, who was a founding member of the State President's political party and a member of the Vilnius City Municipality Council, and the head of State. Such persons inevitably and knowingly lay themselves open to close scrutiny by both journalists and the public at large.'[1]

For the state itself, a double relationship applies. On the one hand, the government has additional obligations to ensure a transparent administrative culture. For example, decisions and their realisation must be clear to citizens. On the other hand, the government is allowed to keep much of its decision-making behind closed doors and there are numerous provisions guaranteeing that discussions, operations and technologies used by government bodies do not have to be made public. The state itself cannot invoke a constitutional right, such as the right to privacy. Also at supranational level, the European Court of Human Rights has ruled that although non-governmental organisations can invoke the Convention, this does not apply to municipalities, provinces or the state itself.

The foregoing means that government bodies themselves are not entitled to invoke privacy, that civil servants *qualitate qua* have to accept additional interference in their private lives and are subject to extra transparency obligations, and that politicians and other public figures have to live with bright spotlights on their private lives. This constellation follows logically from the classic image in which the government has a monopoly on power and can therefore curtail the freedom of citizens, while citizens themselves are relatively powerless. Although this inequality of power still applies and fundamental rights will continue to operate primarily in this light now and in the future, an inverse relationship is increasingly taking shape. Citizens, certainly when they unite in groups and make use of modern technologies, have increasing possibilities to exercise power over politicians, civil servants and the government as such and to control their actions, to address alleged abuses and to influence decisions.

For example, citizens frequently hack into the computers and other devices of politicians and civil servants, for example to steal secrets, blackmail people or manipulate decisions that apply to them. Social media of politicians have been hacked in the past,

1 ECHR, Drakas v. Lithuania, appl.no. 36662/04, 31 July 2012.

such as the Twitter account of Trump, which not only allowed personal data about the politicians and their associates to be obtained, but also enabled citizens to put words to in the mouths of these politicians. The same danger arises with the rise of deepfakes, whereby citizens can pose as ministers or MP to gain access to secret documents, facilities or money, or as a member of another country's opposition in order to obtain information from parliamentarians and frustrate discussions, as already happened in several countries.

In addition to politicians, many civil servants experience additional scrutiny by civilians. An example is arrests made by police officers, that are increasingly being filmed by citizens. These videos are usually distributed on the internet and widely reported and commented on in social media. On the one hand, this exposes abuses, as was most poignantly the case with the fatal arrests in America. On the other hand, situations are taken out of context, for example because parts of the arrest or the escalation of violence that forms the prelude to it are not filmed or broadcast. Moreover, research shows that just the perspective from which a video is filmed has an impact on the viewer's empathy, which is why many police units now have decided to wear bodycams. In countries such as the Netherlands, many other civil servants are now wearing body cams as well, such as employees of the railway services, of municipalities, of governmental inspections on food quality and the environment, of the regional water authorities, etc. Citizens film civil servants while performing their duties, civil servants now film back.

Doxing, making public of private information of officials or asking fellow citizens for these data on online forums, is increasingly used as a threat. Police officers report that their family life is disrupted by the disclosure of their home address, and single police officers who have been doxed reportedly sleep with a weapon on their bedside table. As doxing is on the rise, the police in several countries have called for this phenomenon to be made a criminal offence, which includes asking for the private information of public officials. Politicians, too, frequently have to deal with doxes, for example, to pay MPs ‘a visit’. Even civil servants are increasingly suffering the same fate. In Belgium, the virologist Marc Van Ranst not only was doxed, insulted and threatened online, but had to hide with his family for serval weeks because a civilian had obtained arms and threatened to kill him. The civilian was regarded as a hero or freedom fighter by remarkably substantial groups.

Politicians are also often the victims of online threats, insults and other scurrilous statements. It is estimated that about 10% of all Tweets addressed to female politicians are hateful, misogynistic or simply unlawful. The fact that these insults take place is of course not new, but the volume and the inciting character of such remarks on discussion forums and social media is. Men more often receive death threats, which they more often do not report, which more often does not lead to prosecution, which more often does not lead to conviction.

The state and government bodies also frequently have to deal with data incidents. It is a well-known fact that not only foreign powers look for leaks in data systems, but al-

so clever citizens. Hackers are often out to make money, but increasingly hacks are being carried out to influence decisions or make them public. Platforms like Wikileaks, for example, do not aim to expose a specific wrongdoing, but simply to publish all the documents they can get their hands on, either in full or with minimal editing. The leaks on the Democratic Party in the U.S. allegedly had a big impact on the elections in 2016. Some call this a form of citizen journalism (data journalism) or political activism (leaktivism); the president of the United States calls it terrorism. Wikileaks has had hundreds of followers, such as the the Panama Papers, the Xinjiang Papers, the Offshoreleaks, Bahamas leaks and Paradise Papers.

The disclosure of up to millions of government documents may still be relatively innocent compared to the possibilities for hackers to infiltrate critical government infrastructure. Locks and pumping stations, for example, are relatively easy to hack, which can have catastrophic consequences. Botnets spread by cybercriminals can be used, through DDOS [Distributed Denial-Of-Service] attacks, to bring down government sites at crucial moments, such as during a disaster or catastrophe. Europol also highlights the danger of Deep Fakes, for example when citizens impersonate a minister or politician. Imitating the Minister of Defence to cheat wealthy citizens may be one thing, but it becomes more serious when the fake minister declares war on a neighbouring country.

This problem of 'reversed vertical privacy' will become increasingly problematic in the years to come, but solutions are very few and far between. To grant states fundamental rights to protect itself against citizens would seem a juridical bridge too far, equipping states with more capabilities for controlling citizens while denying them access to monitoring equipment might fuel the distrust in the state, as citizens have to abide by the rules more and more while they have the feeling that 'hypocritical politicians' and governmental organisations themselves are not hold to the rules, and a disarmament on both sides, both states and citizens laying down the technological capacities to monitor each other seems something that no state currently is willing to do. This means that the problem that the legal regime is still rather one-sidedly grounded in the belief that the state has the monopoly of power and that fundamental rights are primarily intended to protect citizens from the use of power by states, while reality is rapidly becoming more complex, will become more intense in the coming years.

Let me turn to this issue. Beate Roessler, author of the standard work on privacy – The Value of Privacy – has recently published a new book on autonomy – Autonomy: An Essay on the Life Well-Lived. In her foreword, Beate critically engages with the question of human nature and the extent to which we can be 'reprogrammed', if we had a program to begin with. In his foreword, Anthony Elliott, author of works on AI – *The Culture of AI: Everyday Life and The Digtial Revolution* – and identity – *Identity Troubles* and *Concepts of the Self* – engages with the question of what empowerment means in the age of AI and Big Data.

The articles section contains four papers. Mariam Hawath engages in a detailed analysis of Article 22 GDPR, on automated decision-making; Christof Koolen engages with

smart devices and smart environments. Both authors assess to what extent individuals' right to control can be respected in the 21th century. Max von Grafenstein offers his second of three articles (the first one published in EPDL 2020/4 on, inter alia, the purpose limitation principle. Finally, Wouters et al. discuss the impact of the GDPR on Big Data health research.

Special mention, as always, should be made of the reports section led by Mark Cole, which is one of the reasons practitioners, academics and government officials mail us to ask whether the new edition of EDPL has been published yet: it provides a perfect overview of all important legal developments on both a European and a national level. After the introduction by Mark (read it), Laura Drechsler discusses the EDPB's Guidance on cross-border data transfers for law enforcement purposes; Carl Vander Maelen analyses the first transnational code of conduct under the GDPR; and Sebastian Zeitzmann sheds light on the Convention of Access to Official Documents by the Council of Europe. Julien Levis and Philipp Fischer discuss developments in Spain in the banking sector; Joost Gerritsen has studied in detail a judgement of a Dutch court on the interpretation of 'legitimate interests'; Giorgia Bincoletto signals an important Italian development, namely that if AI is not sufficiently transparent, data subjects' consent will not be deemed valid; Kristin Benedikt discusses a new act on e-Communication in Germany; Jan Skrabka, based in Czech Republic, signals the complex questions with respect to the implementation of the EU Whistleblowing Directive in his country; and Maria Grazia Porcedda covers the data-driven measures adopted in Ireland in light of the pandemic. A very full reports section indeed, but we also have two reports in the practitioner's corner, led by Axel Freiherr von dem Bussche. Alvaro Moretón and Ariadna Jaramillo delve into the complex issue of voice data and the possibility of full anonymisation and finally, Jens Nebel brings our attention to the matter of administrative fines for neglect of data controller's information duties.

The case note section is also quite full. Belle Beems discusses the case of VQ v Land Hessen, inter alia touching upon the concept of data controller; Paul De Hert and Georgios Bouchagiar are critical of the ECJ's reasoning in the Breyer case; Magda Brewczyńska praises and critiques the case of the European Commission v Spain; Domingos Farinho analyses (yet another) case on the right to access to information; and I myself have written something on the Grand Chamber judgements on the Big Brother Watch and others v. UK and Centrum för Rättvisa v. Sweden.

Finally, the book review section, led by Gloria Gonzalez Fuster, contains two very insightful book reviews. Michalina Nadolna Peeters engages with an edited volume on cross-border data flows and the various complex issues involved, such as concerning extraterritoriality and sovereignty, and Rossana Ducato covers an Italian book by Chiara Angiolini. Italy, since the beginning of the 70ties of previous century, has always been one of the leading countries both intellectually and practically in the field of data protection, and continues to be, as is shown by Rosanna's discussion.

For those interested in submitting an article, report, case note or book review, please e-mail our Executive Editor Jakob McKernan (mckernan@lexxion.eu) and keep in mind the following deadlines:

- Issue 3/2021: 1 July 2021;
- Issue 4/2021: 1 October 2021;
- Issue 1/2022: 15 January 2022.
- Issue 2/2022: 15 April 2022;

I hope you enjoy reading this edition of the European Data Protection Law Review!

Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT) Tilburg University, Netherlands