Editorial

Like any technology, 'Deep Fakes' can be used for better or for worse. Positive applications include producing satire and memes, such as placing Nick Cage in films other than those in which he has starred (not a small number!), making video clips with actors whose lines and presence are generated in whole or in part by a computer, ´bringing to life´ a deceased loved one, a footballer (with permission) asking to support a charity through a video message in all the languages of the world, while in reality he only speaks English, not only translating live texts that someone speaks during a conference call, but also distorting the mouth and lips so that the image and sound are in synch, helping people with identity disorders or amputated limbs to regain a better sense of themselves and to rehabilitate, or projecting cloths offered in a web shop on your own body.

Nefarious applications of Deep Fakes are also well known. The first application of the technology consisted of citizens (men) who 'photoshopped' images of women already in their possession, for example of an ex-girlfriend, or of celebrities found on the internet, on porn actresses in order to generate fake porn movies. Subsequently, this technique has been used for all kinds of applications, such as spreading fake news, committing identity theft to obtain secrets or money, generating fake videos in which people appear to perform illegal acts (for example, sex with a minor) and generating fake speeches by politicians or generals, for example to destabilise a country or a democratic system or to incite hatred or violence.

Deep Fakes may be produced by individuals who have downloaded a free app or purchased a programme, by groups, by organisations and state actors alike. Interestingly, so far, Deep Fakes are mostly applied at the same ´level´, i.e. when citizens use deep fake technology, they tend to target other citizens, states tend to target other state actors, for example, with the aim of undermining that country's democracy, and organisations primarily use deep fakes to outwit other organisations, for example, by extracting trade secrets via a Deep Fake video. This congruence of the type of perpetrator and the type of victim is, of course, not a given. Citizens can also use their newly downloaded app to get Putin to declare war on Lithuania; states can target their own citizens, for example, to discredit political dissidents; and organisations can target customers by using Deep Fakes, either to acquire customers through deception or by offering Deep Fakes as a service.

Although most attention has been drawn to Deep Fakes used to spread fake news or to destabilize a country or a political system, most Deep Fakes are used and produced by citizens, either for satire and memes or, especially, for the purposes of producing fake porn videos. Thus, it fits in the trend of renewed possibilities for citizens to vio-

DOI: 10.21552/edpl/2020/4/3

late the privacy of other citizens: horizontal privacy, which I discussed in my previous editorial. With Deep Fakes, similar questions arise as with horizontal privacy matters in general, especially with respect to the question of who should be the primary norm addressee of legal regulation and the choice between *ex ante* or *ex post* regulation. Deep Fakes, in addition, raise complex material questions for data protection law and for procedural law in general.

The material questions for data protection law are, inter alia, as follows:

1. Are Personal Data Processed with Deep Fakes?

The answer is almost always yes. Even if the data about a person are not correct (e.g. a woman seems to perform certain actions, which in reality she did not), such data is considered personal data. Even an obvious lie, such as 'Boris Johnson is a woman', can be considered personal data because the (untrue) information can clearly be linked to a person, which applies to fake news about citizens as well. Even if someone fabricates and distributes a Deep Fake video of herself, the GDPR will apply, as she will be considered the data subject *cum* data controller. What raises more difficult questions is when a Deep Fake is an amalgam of two or more persons.[1] Although personal data are clearly processed when producing such Deep Fakes, it is unclear whether the Deep Fake itself will be considered personal data for the purposes of the GDPR. If the answer is yes, the two or more persons whose personal data are used may have conflicting interests and views on the legitimacy of such a video.

2. When Would the Household Exception be Applicable?

It seems obvious that if individuals distribute fake videos indoors or in very small and closed (online) circles, this will fall under the GDPR's household exception, whereas if these images are disseminated on the internet and freely available to everyone or large groups of people, this will not be the case. Indeed, both the former Data Protection Directive and the General Data Protection Regulation underline the purpose of processing and emphasise the use and dissemination of personal data: if they remain indoors, the exception will apply. In the Rynes case, however, the Court of Justice took an entirely different approach: a security camera attached to a dwelling filmed part of the public road. There was no doubt that the images were only viewed indoors, by the owner of the house herself, and were not distributed. Nevertheless, the Court of Justice indicated that the exemption did not apply because the images were collected from the public domain: it was the source of the personal data, not their use, that was determinative for the Court. If this approach is applied to Deep Fakes, the question is whether if personal data are collected from an open source but the Deep

1 Marwan Albahar and Jameel Almalki, 'Deepfakes: Threats and Countermeasures Systematic Review' (2019) 97 Journal of Theoretical and Applied Information Technology, 22, 3242-3250.

Fake itself is only used/shown in private and closed circles, the exemption would apply.

3. How do Deep Fakes Relate to the Purpose Limitation Principle?

Suppose a person places a professional photo online on the website of her employer, that photo may in principle not be reused for a fake video (provided the GDPR applies, see questions 1 and 2), unless a new and legitimate processing ground is found (see question 5).

4. How do Deep Fakes Relate to the Data Quality Principle?

The GDPR states that personal data should be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'. Although there is considerable discussion about what exactly should be considered correct or accurate and how big the duty of care of the data controller should be in this respect, it is difficult to see how this principles can be respected with Deep Fake technology, perhaps with the exception of when a conflict between the freedom of expression and the right to data protection arises and the former prevails.

5. What is a Possible Processing Ground for Deep Fakes?

Of course, if someone disseminates a Deep Fake of herself, there is consent, and the same applies when friends or family agree with a Deep Fake of them being produced. In addition, when fake videos are produced and used in professional relationships (e.g. of an actor for the purpose of producing a movie), there may be a contractual relationship. However, the vast majority of Deep Fakes distributed by citizens concern non-consenting individuals and are produced and distributed without their permission or knowledge. The only possible basis in such cases is if the processing of personal data is 'necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.' Such will obviously not be the case when unlawful activities are performed (fake news, fake pornography, identity fraud, etc.). But perhaps, it may offer a pathway to Deep Fake memes or satire, because in general, little harm is done to the data subject and engaging in satire it is in itself justified.

6. What is a Possible Processing Ground for Deep Fakes Making Use of Sensitive Personal Data?

Deep Fakes that show explicit sexual content, criminal activities or political beliefs or statements will fall under the regime of sensitive personal data; processing these data,

in principle is prohibited. With the exception of Deep Fakes for which explicit consent has been given or those that are developed in contractual relationships, none of the grounds given in Article 9 paragraph 2 GDPR seem to offer solace for Deep Fakes produced by citizens about other citizens. It seems unlikely that, when Deep Fakes make use of pictures available on the internet, courts will allow citizens to rely on the exception that data have been made manifestly public, because they are not made public with the purpose served by Deep Fakes and because what is fake in Deep Fake video's will often precisely concern the sensitive data (e.g. a person appears to perform sexual activities that she did not; Putin appears to declare war on Lithuania, but in reality did not; a dissident appears to engage in criminal activities, which he did not perform). Consequently, these data have not been made manifestly public before, they are produced through the Deep Fake.

7. How do Deep Fakes Relate to the Freedom of Expression?

The GDPR offers countries the possibility of laying down exceptions to the data protection regime when data are processed in the context of freedom of expression - a fairly broad doctrine that includes the right to disseminate and receive information and the right 'to shock, offend and disturb'. It will be interesting to see to what extent courts will deem fake videos to fall under this doctrine and how it would resolve conflicts of these two rights.

8. How Can the Obligation to Inform Data Subjects be Met?

The GDPR contains the obligation to inform data subjects that their data are being processed, either immediately when data are acquired from the data subject directly, or as soon as possible after the processing has started, when data are obtained indirectly, for example through harvesting open sources. Although there is an exemption to the obligation when data are acquired indirectly and informing the data subject would involve a disproportionate effort, even in these cases, the data controller must take alternative measures, such as providing all relevant information, including her identity, the purpose of data processing and the ground for processing, on a public website.

In addition to these material questions with respect to the data protection regime that are raised by Deep Fakes, there is a procedural element. Whether Deep Fakes are regulated and addressed through criminal law, data protection law, civil law or through softer law and self-regulation, and whether rules are enforced by citizens, by Internet intermediaries or by the state, there will always be a question with respect to truth, authenticity and verifiability. Who is to say that images or audio fragments that are shared on the internet – for example of a person engaging in illicit activities – are real? Should the police investigate and how? What if a case goes to court, who will have the burden of proof to show that the video either is or is not authentic? What should be the standard of proof? What if an Internet provider is confronted with citizens with conflicting claims or if citizens themselves produce material in court proceedings, for ex-

ample to exonerate them? If Deep Fakes would become more and more realistic and the use of this technology would continue to mushroom as it does now, would the veracity of all audio and video fragments become equivocal? If it is impossible to verify technically whether a video has been fabricated or not, how do you prove that you did not do something which you did not do? And what if material is not released immediately, but is 'archived' and only released after a person's death (e.g. a compromising video to ruin her moral legacy); who can then dispute the authenticity of a video and on what grounds? [2]

This issue opens with two forewords, one by Kieron O'Hara and the other by Neil Richards and Woodrow Hartzog, on what could be called the 'moral turn' in privacy and data protection literature. This turn has been advocated, especially in the Anglo-Saxon world, and emphasizes the need for trust and reciprocal relationships, in which there are moral obligations that go beyond the strict legal rules and obligations. Mostly, these trust relations focus on the role of the intermediary and its obligations vis-à-vis the citizen. A classic example is the notion of the information fiduciary developed by Jack Balkin; in addition, I have argued that organisations with data power have moral (virtue) duties vis-à-vis data subjects in my book *Privacy as virtue*. I'm very proud that three authors that are currently on the forefront of this debate have been willing to contribute to this issue of EDPL. Kieron O'Hara writes about Data Trusts, or organisations that manage the data of its trustees. Kieron explores several approaches to the Data Trust model and discusses potential problems connected to each of those. Neil Richards and Woodrow Hartzog argue for a relational turn in privacy and data protection law, stressing that the goal of data protection law should be to promote trust in the digital environment. This, they argue, would have the added benefit of focussing directly on power imbalances in relationships rather than indirectly through data rules.

There are four great articles in this edition. Daniel Groos and Evert-Ben van Veen question the EDPB's stance on anonymous data and argue for a different approach in which principles of the rule of law and legal certainty are embedded. Maximilian von Grafenstein has written the first in a series of three articles on the purpose limitation principle, in which he discusses how a re-connection of data protection law to concepts of risk regulation may help clarify the ambiguous object and concept of protection. Valeria Ferrari analyses the private-public partnerships that exist between law enforcement organisations and banks in the fight against terrorist financing and anti-money laundering. She evaluates how privacy and law enforcement priorities interplay in determining the governance of financial data and concludes that privacy-enhancing payment methods should be encouraged and legitimised. Michael Cepic and Mariana Rissetto discuss the security requirements for cloud computing infrastructures, in particular in the medical domain. They map the various legal requirements currently in place and evaluate them.

2 Riana Pfeferkorn, ''Deepfakes' in the Courtroom' (2020) 29 Boston University Public Interest Law Journal, 2.

As always, special mention should be made of the reports section led by Mark Cole. This time perhaps even more so, because of his introduction to this section, in which gives a beautiful overview of the past year, the life events that have happened as well as many of the important developments in privacy and data protection law. The reports section itself contains two reports on EU Member States, namely one by Giorgia Bincoletto on the Italian DPA's fine against Vodafone and another by Niki Georgiadou and George Kakarelidis on the tension between medical privacy and public safety in Greece. There are also two reports that cover important developments on EU level, namely one by Christina Etteldorf on the ePrivacy Regulation and another by Giorgia Bincoletto on the EDPB guidelines on data protection by design and by default. In the GDPR implementation series, David Ciliberti covers Malta. And finally, the Practitioners Corner include two contributions. Amanda Antonely Bispo discusses the PSD2 framework and Maria Mitjans Serveto presents an overview of empirical insights as to explanation in News Recommender Systems.

For the case note section of this edition, special thanks to Federico Ferretti, who has replaced Maja Brkan and Tijmen Wisman as editor of this section. This edition includes four interesting case notes. Virgilio Emanuel Lobato Cervantes covers the ground breaking ruling of the Court of Justice in the Schrems II case, which needs no further introduction. Elena Kaiser reviews the judgement of the Court of Justice on the notion of free, specific and informed consent. Patsy Kirkwood analyses a judgement by the European Court of Human Rights on the conflict between freedom of expression and the right to privacy. Finally, Bruno Ricardo Bioni, Renato Leite Monteiro, Rafael A. F. Zanatta and Mariana Rielli discuss a Brazilian case that is of interest to a broad audience because the Brazilian Supreme Court has recognized data protection as a fundamental right for the first time.

The book review section, led by Gloria Gonzalez Fuster, includes a review of three recent and ground breaking books. Andreas Ebert gives an overview of Virginia Dignum's book on responsible AI, Maria Magierska reviews Of Privacy and Power written by Farrell and Newman and Gloria Gonzalez Fuster herself gives a detailed account of the edited volume by Taylor and colleagues on the meaning of the concept of Data Justice in the current pandemic.

I want to thank the reader of EDPL for continuing to actively engage with me, the editors and authors; the authors of the numerous contributions to the four issues of EDPL this year for their continuous stream of intellectually stimulating articles, reports, case notes and book reviews; the editors and associate editors of the journal, for managing the various sections, activities and projects under the EDPL umbrella; and of course Jakob McKernan, the backbone of this journal and the linking pin between the publishing house, the editors, the authors and the readers of this journal. Finally, on a sad note, Tijmen Wisman will step down as case note editor as per next year. I want to thank Tijmen for his years of hard work and commitment to this section; together with Maja, he has ensured that this section is vibrant, topical and of a very high quality. Luckily, Tijmen will remain a member of EDPL editorial board. I wish everyone all

the best for the coming year and hope that the spirit of love will guide and protect you in 2021.

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

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

Bart van der Sloot