Editorial

The EU is seen as the world leader in terms of the regulation of data and technology, and perhaps regulation in general, and rightly so. It has recently adopted the General Data Protection Regulation,[1] the Law Enforcement Directive,[2] the Open Data Directive[3] and the Regulation on the free flow of non-personal data,[4] just to name a few. In addition, the Data Governance Act,[5] the AI Act,[6] the e-Privacy Regulation,[7] the Digital Services Act[8] and the Digital Markets Act[9] are currently under discussion. Then there are various policy initiatives, such as the European Strategy for Data,[10] the European Health Data Space,[11] the White Paper on AI,[12] the EU Open Data initiative[13] and the EU Smart Cities Market Place.[14] What the EU lacks in military power, it compensates in bureaucratic power. Its capacity to develop comprehensive legislative frameworks on any economic, social or technical issue is unparalleled. While China might exert its global power through financial means, and the U.S. may impose its dominance with the use of force, the EU will be able to rule the world through its regulatory force. The Brussels effect – the effect that EU legislation will be adopted by companies around the world and be transplanted to many national legal regimes across the globe – is not limited to the GDPR. The EU may become the world's regulatory force.

DOI: 10.21552/edpl/2021/3/3

1 Regulation 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)

2 Directive 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

3 Directive 2019/1024 of the European parliament and of the council of 20 June 2019 on open data and the re-use of public sector information, pe/28/2019/rev/1

4 Regulation (2018/1807 of the European parliament and of the council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (text with eea relevance.)

5 Proposal for a regulation of the European parliament and of the council on European data governance (data governance act), com/2020/767 final

6 Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts com/2021/206 final.

7 Proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/ec (regulation on privacy and electronic communications) com/2017/010 final - 2017/03 (cod)

8 Brussels, 15.12.2020 com(2020) 825 final 2020/0361 (cod) proposal for a regulation of the European parliament and of the council on a single market for digital services (digital services act) and amending directive 2000/31/ec (text with eea relevance) {sec(2020) 432 final} - {swd(2020) 348 final} - {swd(2020) 349 final}

9 Brussels, 15.12.2020 com(2020) 842 final 2020/0374 (cod) proposal for a regulation of the european parliament and of the council on contestable and fair markets in the digital sector (digital markets act) (text with eea relevance) {sec(2020) 437 final} - {swd(2020) 363 final} - {swd(2020) 364 final}

10 Brussels, 19.2.2020 com(2020) 66 final communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions a European strategy for data

11 See, <https://ec.europa.eu/health/ehealth/dataspace_en>.

12 Brussels, 19.2.2020 com(2020) 65 final white paper on artificial intelligence - a European approach to excellence and trust

13 See, <https://data.europa.eu/data/datasets?locale=en>.

14 See, <https://smart-cities-marketplace.ec.europa.eu/>.

At the same time, technology regulation in the EU seems like a game of musical chairs at times. Although the EU's legislative proposals are avant-garde and extensive, at the same time, they lack specificity. Take the GDPR. What does it actually say? Not much more than the obvious. Only gather data that you need, specify a purpose before you gather data, delete the data when you no longer need them, store the data safely and confidentially, etc. It does not provide clear standards (how long can data be stored; when can data be shared with third parties; etc.), and as a consequence, in and by itself, the GDPR is unable to give much guidance on modern data processing operations. This holds true for the many procedural requirements in the GDPR, such as the obligation to do a DPIA, to appoint a DPO, to adopt a data protection policy, and so forth, as well.

Consider the following. A Latvian university, a Brazilian university, an Austrian law enforcement authority and a sewage company based in the UK set up a consortium to assess whether it is possible to monitor sewage material for traces of Covid19 and drug production/consumption. Just some questions with which they will struggle: Should each party have its own legitimate ground for processing personal data (e.g. the law enforcement authority basing itself on the law enforcement directive, the Latvian university on 6(e) GDPR, the sewage company on 6(f) GDPR, etc.) or can they chose one legitimate ground? Can they store data in one dataset or should the data be segregated per party, as there might apply different grounds for processing, meaning that not all parties can access all data that are gathered, and different standards for data storage? Can the police share general findings with European partners? If sewage samples are taken under a specific building, do these qualify as personal data? The GDPR does not give any guidance on these types of questions, while most modern-day data processing initiatives regard these types of complex consortia and processing techniques.

The GDPR is not alone in its relative vagueness. Take the proposed AI Act. It sets many rules on preventing and mitigating risks and harms. But what this means in practice is left unspecified. Uniquely, there is an article that sets rules on the prohibition of AI systems (article 5), but these are again framed in general terms such as 'an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm'. But when is such the case? When does an AI system exploit 'any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm'? No guidance is given on this point, no specific technique or application is referred to.

Rightly so, it could be argued, because regulation should be technology neutral. Perhaps this is true, although there also arguments against technology-neutral regulation. In any case, it is clear that the AI Act is not technological neutral, it mentions specific applications, such as deep fakes, on several occasions. Article 52 paragraph 3 specifies: 'Users of an AI system that generates or manipulates image, audio or video con-

tent that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated.' This provision is emblematic for the EU's approach to regulation; it doesn't set clear prohibitions or standards, but lays down general and open norms; if it does make reference to specific technologies, it is to lay down procedural and bureaucratic requirements. This means that a technology or application is allowed, as long as it adheres to these standards. The Act does not prohibit deepfakes, nor does it, for example, set a moratorium on the use of facial recognition systems in public places.[15]

This regulatory approach has several drawbacks. For example, although deepfake-technology can certainly be used for positive purposes, some 96% percent of the deepfakes concern non-consensual porn (usually by superimposing the face off an ex-lover or celebrity on an existing porn movie). Add to that the uses of deepfakes for identity theft, inciting hatred among groups and spreading fake news, and it is clear that almost all deepfakes are used for unlawful purposes.[16] But the EU does not prohibit this technology, or, for example, ban the product from the consumer market. It only lays down a transparency obligation, which is inherently vague. (1) The provision regards all manipulated content; the problem, however, is that, depending on your definition of manipulation, every communication technology distorts. Video-services have built in tools that equalize skin tones, audio services filter out high pitched tones automatically, etc. The estimation is that in 5 years' time, more than 90% of all online content will be manipulated in some form or another. Importantly, the AI Act also refers to manipulated content about objects, places and events. Does this provision also apply to an AI generated picture of the sun with a smiley face? (2) The provision only holds that the user should disclose that the content had been manipulated: but to whom should it disclose such information? The general audience; the person depicted; the platform on which it is posted? (3) It is the user of the AI system that bears the obligation to disclose information as to the manipulation of the media; how should it do this? Via meta-content or in the content itself? How big or small should the explanation be? What should that information entail: 'this content has been manipulated' or a description of what has been manipulated? Presumably, it regards the metadata of the content as recital 70 specifies: 'by labelling the artificial intelligence output accordingly and disclosing its artificial origin.' But then the question is, will users indeed label a funny deepfake video's they made of their aunt, even if they knew how?

Presumably, this provision, as well as many others, will only add to the bureaucracy and will not have the effect that the problematic deepfakes are actually addressed. But again, it could be argued that most if not all of the problematic deepfakes are already prohibited through law, e.g. disseminating nonconsensual porn, identity theft, inciting hatred, etc., are all matters typically regulated through criminal law. That is true, but

15 See, <https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en>.

16 See, <https://www.europol.europa.eu/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf>.

it is also shows what might be the problem with this type of regulation: it adds little, or worse, because companies and citizens can claim that they have adhered to the procedural requirements of the AI Act, they may believe or claim that they have acted legitimately.

The problem is that deepfake-technology is democratized and that millions of EU-citizens are already experimenting with producing fake content. It is impossible for any regulator, public prosecutor or internet intermediary to check all digital material and assess whether content is fake or not, whether consent was given (consent can obviously also be faked, deepfake technology allows a user to let the depicted person say 'I consent to this material being spread on the internet') and take action when necessary. Yet the same regulatory strategy is chosen with respect to other technologies. Take spy products. Obviously, even spy products can be used for bonafide applications such as when journalists want to take secret recordings or when citizens want place spyware to catch perpetrators at their premises. Yet these products are often explicitly advertised to consumers as tools that allow them to spy on their partner, their ex-lover or their employee. Of course a mini-camera explicitly advertised as easy to hide in the cap of a shampoo bottle can also be used for other purposes than for secretly filming a person in the shower; of course an audio recording devise explicitly advertised to listen in on bedroom conversations through walls can also be used for finding out whether there is a mouse in the cavity wall; of course spy apps that allow you to read every e-mail, listen in on any telephone call, and put the devise in recording mode from a distance can also be used for bonafide purposes; of course. But it is clear that by far most cases in which these products will be used will be for malafide means. The problem, again, is that under the current regulatory approach, citizens are able to freely acquire those products and use them. Only when they are used for unlawful activities and only if this becomes known to any party other than the person using the products (which is of course not her intention) can legal action be taken.

The choice for open norms and ex post regulation is not be a problem in and by itself. The EU could very well adopt general principles, abstract duties of care and procedural requirement, if national legislators would provide further detail as to the the meaning and interpretation of these vis-à-vis specific technologies, applications or contexts. But the national implementation acts have generally refrained from doing so, though there are specific prohibitions and clear red lines here and there. This again would not be a problem in and by itself if Data Protection Authorities would take up that role. But DPA's are generally hesitant to adopt concrete guidelines and adopt moratoria on their own. They often point to the EDPB, as most legal questions play a role in other countries as well and there should be a level playing field throughout the Union. In addition, DPAs often do not have the manpower to give detailed advice to companies or institutions with questions about what is and what is not legitimate; rather, they sanction illegitimate data processing operations ex post, using the stick rather than the carrot. The EDPB has adopted quite a number of opinions, but these mostly regard frameworks proposed by the EU, legal agreements for the transfer of data or the lists for mandatory Data Protection Impact Assessments adopted by the DPAs. There are but a

few opinions that do discuss concrete applications or technologies and how the general principles should be interpreted in those concrete contexts. But again, this would not be a problem in and by itself, if the possibility to set up codes of conducts by associations would be regularly used. Through such codes, organizations can agree on specific rules and standards for their own sector, such as the national association of universities. Such code could specify standards for, inter alia, international consortia, for consortia with private sector partners, for obtaining a legitimate ground, for sharing data between the consortia partners, for data storage terms, etc. But surprisingly few associations have so far adopted such codes of conducts, among others, because they are weary of the paperwork and the fact that they will be responsible for the oversight of and compliance with the rules, and have to set up an independent institution that is responsible for issuing judgements on complaints by data subjects or on other disputes that may arise. Rather than taking up that role themselves, they stress that the national or EU regulator should set up clearer guidelines and rules for specific sectors.

The loser of this game of musical chairs is legal certainty. Data controllers often do not know whether their internal policies and activities will be deemed in conformity with the GDPR by the DPA. Data subjects don't know concrete standards either and are thus left in the dark about whether the processing of their data in concrete circumstances is legitimate or not, until they have heard the decision of the DPA or judge in her specific case. Because there are no ex ante prohibitions nor concrete rules and guidelines for concrete technologies and contexts, Data Protection Authorities are overwhelmed by requests and cases. And the EU Commission often loses cases against the internet companies because the EU Court of Justice adopts another interpretation of the rules than it did.

Europeans used to mock Americans for their sector specific approach to data protection; they had informational privacy standards for specific domains, such as laws for the protection of online privacy of children, laws concerning privacy protection in the health care sector, laws regarding data processing in light of credit reporting, etc. We, instead, had an omnibus law, that applied to all data processing activities irrespectively. Thus, there were no legislative gaps and no discrepancies between the various legal instruments. European data protection legislation is, of course, still miles away from any other legislative regime around the word and the EU and the Court of Justice have taken immense steps to ensure that citizens are protected against large internet companies.

Yet the more diverse the type of data processing techniques become, the more diverse the parties that have access to the technologies and the more diverse the goals for which they are put to use, the less an omnibus regulation seems the right type of regulation. In the 1990s, there were still relatively few data processing techniques available and there were relatively few parties with access to them. Now, not only big corporations and governmental organizations, but virtually everyone has access to advanced data processing technologies. These technologies may serve a variety of means. Medical institutions that do total genome analysis, for example, are in no way com-

parable to citizens that use drones and spy products; the way in which in smart cities, private-public partnerships use data analytics for nudging is in no way comparable with how companies extract information from public sector information that has be made available for re-use in aggregated form. The more disparate the data processing landscape becomes, the more the question becomes relevant: should we not rather work with sector specific and technology specific regulation? The AI Act may be seen as a first step toward that approach, but a baby step.

It is my pleasure to introduce the third edition of EDPL 2021. Mireille Hildebrandt opens this edition with reflections on the question of equal treatment, bringing the AI debate of discrimination and fairness back to a human debate. AI systems confront us with our own biases and systemic discriminatory world; it is our problem to solve. Sandra Wachter picks up on the same theme: 'if we see AI as a mirror of society that shows us where inequalities exist, we can use this knowledge as a starting point to rethink our selection strategies and criteria for housing, insurance, parole, education, hiring, and other critical areas of life.'

There are three articles in this issue. Maximilian von Grafenstein offers his third and final article on the role of purpose limitation in EU law, Alexandra Giannopoulou analyses the role of data protection by design and blockchain under the GDPR and Niels Vandezande & Jos Dumortier offer reflections on one of the most topical discussions in the data protection community, and that is how for law enforcement authorities can go in the fight against Covid-19.

The report section led by Mark Cole is as always packed with insightful discussions of recent developments throughout the EU. First, Mark offers his own reflection on these developments, then there are three country reports on the fines issued by the Dutch DPA against TikTok (Eva Lievens), on the sanctions issued by the Italian DPA (Giorgia Bincoletto) and the Belgian DPA's new policies (Thomas Dubuisson), there is one report on a recent EDPB decision (Lisette Mustert), one practitioner's report on Article 32 GDPR (Annika Selzer, Daniel Woods and Rainer Böhme) and finally a report on India's new IT Rules (Ashit Kumar Srivastava). Bram Visser has written a case note on Berlizev v. Ukraine and I myself have written something on an ECJ case that might have farreaching consequences for the legal instruments that promote the reuse of Public Sector Information. Finally, there is one book review in the section led by Gloria Gonzalez Fuster, namely on a book by Skinner-Thompson. The book review is written by Julien Rossi and he warns us about, among other things, European complacency.

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 4/2021: 1 October 2021;

- Issue 1/2022: 15 January 2022;

- Issue 2/2022: 15 April 2022;
- Issue 3/2021: 15 July 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