Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Internet service providers as law enforcers and adjudicators. A public role of private actors

*Stanisław Tosza**

Associate Professor in Compliance and Law Enforcement, Faculty of Law, Economics and Finance, University of Luxembourg, 4, rue Alphonse Weicker, L-2721 Luxembourg

ARTICLE INFO

Keywords:
Enforcement
Compliance
Internet service providers
Private actors
Illicit content
Liability exemption
E-commerce
Digital services act
Terrorist content online regulation
Digital evidence
Digital capitalism

ABSTRACT

Private actors have become increasingly involved in the law enforcement process in recent years, taking up more proactive roles and being increasingly engaged in choices between conflicting rights and freedoms. The development and spread of information and communication technology (ICT) created a set of conditions in which the participation of private actors (service providers in this case) appears to be a necessity. These conditions include, for example, a lack of physical borders for ICT technologies, the speed and width of the spread of information on the Internet, as well as the growth of technological behemoths. The resulting reaction can be seen in various sectors, such as combatting illicit content online or gathering digital evidence. While executing these roles they may be compelled – de jure or de facto – to make value judgments which traditionally belong to the public authorities. At the same time the legal framework is either lacking or it does not fully cover the consequences of this fundamental paradigm shift, to the detriment of the authorities, private actors and persons concerned.

The objective of this article is to examine the most important features of these developments and analyse resulting key legal problems. The author demonstrates that the legal landscape of cooperation between law enforcement and service providers must be rethought and offers a direction for this reflection.

1. Introduction

Private actors have become increasingly involved in the law enforcement process in recent years, taking up more proactive roles and being increasingly engaged in processes affecting rights and freedoms. The suspension of the Twitter account of the then President of the US, Donald Trump, followed by his "deplatforming" on other services, has become a prominent example which quickly widened public awareness as to how much the role of service providers as quasi-public actors has grown.

The involvement of private actors in enforcement, however, is not such a recent development.[1] Anti-money laundering policies have been imposing due diligence duties on cer-

[1] Andrew Ashworth analyses the increasing imposition of positive duties on individuals and organizations and categorises them into duties to report, duties to prevent and duties to protect, see: "Positive duties, regulation and the criminal sanction", (2017) 133 *Law Quarterly Review* 606.

* Corresponding author.
E-mail address: stanislaw.tosza@uni.lu

https://doi.org/10.1016/j.clsr.2021.105614

tain entities since the early 1990s.[2] The increasing use of plea bargaining in corporate liability cases has created space for private investigations.[3] However, the development and spread of information and communication technology (ICT) created a set of conditions in which the participation of private actors (Internet service providers (ISPs)) in law enforcement has become a necessity, while also potentially creating space and need for a much more proactive role for them. These conditions include, for example, a lack of physical borders for ICT technologies, the speed and width of the spread of information on the Internet, as well as the growth of technological behemoths. As a result private actors set up rules, enforce them and become arbiters between conflicting rights and freedoms, a role that traditionally pertains to the public domain. This is a real paradigm shift in the relationship between the private and public sphere with significant consequences for public policy, private actors and people concerned by their decisions, while the available legal framework does not reflect or regulate these new power dynamics.

Two areas provide prominent examples of this trend. The first one is content moderation and combatting illicit content online, where service providers play a crucial role in monitoring and taking down illicit content. This role is, on the one hand, increasingly the subject of legislation and regulation and, on the other hand, service providers actively take it up. Both approaches are not without controversy, particularly where they are compelled to choose between freedom of expression and other rights. The second area is gathering of digital evidence for criminal investigations, where the cooperation of service providers has become a necessity for law enforcement authorities seeking access to this type of evidence. The often cross-border aspect of access to data has created conditions in which it is for service providers to assess the legality or proportionality of requests, where their role becomes similar to that of public entities.

While some aspects of these problems are subject to extensive analyses within their domains,[4] it is argued here that this new role for private actors needs to be subject to more extensive scrutiny and to a more comprehensive reflection in general. This reflection is necessary as this paradigm shift will continue to generate problems of two kinds. Firstly, new areas will be increasingly subject to this phenomenon. An example is the growing use of AI technology in public enforcement offered by private companies, where the mechanism cannot be fully explained or subject to the scrutiny deemed necessary for public decision making (the black-box problem). Secondly, a complex set of tools limiting the possibilities for abuses of power has been designed for the public sector. These solutions do not apply, or may be unsuitable for the role which private actors play. An example could be the risk of corruption of service providers' employees who are responsible for taking decisions of a public nature.

The first objective of this article is to demonstrate how private actors have evolved into playing this more proactive role in enforcement and how they also play the adjudicative role, by using the example of the area of content moderation (Section 2) and gathering of digital evidence (Section 3). The second objective of the article is to examine the problems resulting from private actors taking up these public tasks (Section 4) and the factors that create conditions for this phenomenon to occur and increase in intensity (Section 5). As a result a deeper rethinking of the role of private actors in enforcement, in view of these developments, will be advocated for (Section 6). Some concluding remarks will show the broader perspective of this reflection (Section 7).[5]

The paradigm shift in the role of private actors that this article analyses is not only relevant for the legal domains in question, but is also part of two larger fundamental reflections. The first one stems from the dissatisfaction with the current shape of capitalism and the role of corporations, exacerbated by the 2008 financial crisis and its unsatisfactory aftermath. Should such corporations be driven only by profit maximisation and serving their owners' gain or should they benefit other stakeholders and society as a whole?[6] The second one stems from the dissatisfaction with the way in which digital (or surveillance) capitalism has evolved.[7] While the outcomes of these two reflections will shape the future of the economic and social system, the answers to the questions put forward in this article will shape the functioning of the law enforcement.[8]

2. Content moderation and illicit content online

In May 2020 Facebook announced the composition of the initial group of 20 members for its Oversight Board (FOB), known also as the "Facebook Supreme Court",[9] which will eventually grow to 40 people. The board includes Helle Thorning-

[2] Benjamin Vogel, Jean-Baptiste Maillart, *National and International Anti-Money Laundering Law*, Intersentia 2020.

[3] For instance, in the course of the investigation against Siemens for corrupt practices, the company's cooperation was a significant mitigating factor: "Statement of Siemens Aktiengesellschaft: Investigation and Summary of Findings with respect to the Proceedings in Munich and the US", Press Release of 15.12.2008, 7. See also: Karl Sidhu, "Anti-Corruption Compliance Standards in the Aftermath of the Siemens Scandal", (2009) 10 *German Law Journal*, 1343.

[4] E.g. the proposal for the Digital Service Act and the E-evidence initiative, see below (Sections 2 and 3 respectively).

[5] This article takes the European perspective as it looks at the problem from the perspective of the European human rights framework as set up by the European Convention of Human Rights and the Charter of Fundamental Rights of the European Union. Some examples of US law will also be given.

[6] Jean Tirole, *Economics for the Common Good*, Princeton University Press 2017.

[7] Shoshana Zuboff, *The Age of Surveillance Capitalism*, Profile Books; Julie Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, OUP 2019.

[8] A similar trend has been identified as regards private actors taking over regulatory roles. See on that e.g. Diane Rowland, Uta Kohl, Andrew Charlesworth, *Information Technology Law*, Routledge 2016, Chapter 3: Intermediary Liability, 73-125; Jan Trommer, *The Responsibility of Private Actors in the Internal Market Private Actors taking over?*, EUI PhD 2017, available at: https://cadmus.eui.eu/handle/1814/45246.

[9] evelyn douek, "Facebook's Oversight Board: Move Fast with Stable Infrastructure and Humility", (2019) 21 North Carolina Journal of Law & Technology, 3.

Schmidt, former Prime Minister of Denmark, Alan Rusbridger, former editor-in-chief of the UK newspaper, *The Guardian*, and Tawakkol Karman, a Nobel Peace Prize winner and other experts, including some lawyers.[10] This is a response to many calls, issued notably by civil society organizations in an open letter,[11] and by the UN Special Rapporteur, on the promotion and protection of the right to freedom of opinion.[12] They called on Facebook to provide some sort of mechanism of accountability for decisions to remove content and to provide a chance of independently reviewing such decisions. The FOB would be a "new model of content moderation" allowing users to appeal content decisions regarding Facebook and Instagram to an independent body. The FOB would function independently from Facebook, and would also be underwritten by an irrevocable trust of $130 million which would fund its operations.[13]

Expectations as to the FOB and its limitations have been already subject to scholarly scrutiny.[14] Regardless of its eventual success or failure, the initiative as such, and also the need for it, is an excellent demonstration of the necessity for private actors to take part in law enforcement, of their proactivity and of their adjudicative power.

Digital technologies, in particular Facebook, created digital public space which is crucial for political, economic and cultural life within countries as well as globally,[15] while at the same time giving enormous possibilities for abuse, incitement to violence and spread of misinformation.[16] The latter aspect results in the need to control the content, which is technologically or practically cumbersome, but even more so normatively. The normative difficulties arise from the fact that the need to act might not only concern illicit content, but also content which is *per se* legal, while still being harmful and worth removing. Providers see themselves obliged to provide community guidelines, which need to strike a balance – *in abstracto* – between protection of the freedom of speech and protection of other values.[17] Even for the most straightforward illegal content, the scope of legal and illegal may differ amongst countries, which creates difficulties for a global provider such as Facebook. Striking the right balance for the content which is not illegal as such is even more difficult, in particular in an increasingly polarised world.

Once the rules are established, they need to be enforced, which also becomes the responsibility of the providers. In the process, providers need to solve – *in concreto* – conflicts between freedom of expression (or freedom of speech) and other rights. As will also be explained further in this section, at all these stages private actors perform tasks which make them similar to public actors, by assuming the roles of rulemaking, enforcement and adjudication.

These roles have been increasingly imposed on private actors by law. However, the platforms also take initiatives and occupy this regulatory, adjudicative and enforcement space, as the Facebook Oversight Board well exemplifies. The fact that legislation imposes the duties does not necessarily mean that it provides sufficient guidelines as to how to solve the above-mentioned conflicts, which again leaves space for private actors to exercise a public function. We can observe these developments when examining the combatting of illicit content in the European Union.

From the early stage of the development of platforms as we know them now, hosting providers were already profiting from the conditional liability exemption,[18] provided for in Article 14 of the e-Commerce Directive.[19] Hosting information society service providers are not liable "for the information stored at the request of a recipient of the service, on condition that (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information". Another component of this legal framework is the prohibition of a general monitoring duty. It is of great importance as it protects providers covered by Article 14 from being obliged in general "to monitor the information which they transmit or store, [… or to] actively […] seek facts or circumstances indicating illegal activity" (Article 15 (1)). *A contrario*, specific obligations are allowed.

As the exemption depends on lack of knowledge, notification of the infringement obliges the service provider to act. This way Article 14 of the e-Commerce Directive has also be-

[10] https://www.oversightboard.com/news/announcing-the-first-members-of-the-oversight-board/.

[11] https://www.hrw.org/news/2018/11/14/open-letter-mark-zuckerberg; The letter also refers to the Santa Clara Principles available at: https://santaclaraprinciples.org.

[12] David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/HRC/38/35.

[13] https://www.oversightboard.com/news/announcing-the-first-members-of-the-oversight-board/

[14] See for instance: evelyn douek, "Facebook's Oversight Board: Move Fast with Stable Infrastructure and Humility", (2019) 21 North Carolina Journal of Law & Technology; of the same author, "What Kind of Oversight Board Have You Given Us?", U. Chi. L. Rev. Online, published on 11 May 2020; Kate Klonick, "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression", (2019) 129 Yale L. J., 2418.

[15] Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, Yale University Press 2018, 3-8.

[16] The 2020 US Presidential elections are a case in point, which led to more intense interventions of major service providers, flagging posts containing misinformation on the validity of the election and eventually blocking the account of President Trump on the day of the attack on the U.S. Congress. Abby Ohlheiser, Eileen Guo, "Twitter locked Trump's account. Insiders say it needs to go further", *MIT Technology Review*, 6 January 2021.

[17] In her recent article evelyn douek tells the story how Facebook was struggling with finding the right policy as regards the ads for face masks in the wake of the COVID-19 emergency: "Governing Online Speech: From 'Posts-As-Trumps' to Proportionality and Probability", available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3679607, (forthcoming in: (2021) 121 *Columbia Law Review*, No. 1) 2-3.

[18] Hosting is "an information society service [… consisting] of the storage of information provided by a recipient of the service". Articles 12 and 13 also provide for exemption for mere conduit and caching providers respectively.

[19] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178/1.

come the basis for the 'notice-and-action' mechanisms. These procedures have become a crucial element of policies against illicit content in various sectors and in national law, often including voluntary agreements with service providers. For instance, the European Commission agreed with Facebook, Microsoft, Twitter and YouTube a "Code of conduct on countering illegal hate speech online" in May 2016. This code – joined later by some other providers (Instagram, Google+ and Snapchat)[20] – is meant to help users to notify illegal hate speech in these social platforms and to help and provide coordination with national authorities. The Code contains commitments regarding the notice-and-action procedure. The companies have committed to reviewing the majority of requests to remove content in less than 24 h and to removing the content if necessary.[21] Another example is the "Memorandum of Understanding on the sale of counterfeit goods via the internet".[22] The participants in the Memorandum (which include, inter alia, Amazon, eBay, Facebook Marketplace as well as Adidas, Hermès, Nike and Philip Morris)[23] commit to offer efficient and effective notice-and-action procedures, while the rights owners commit to use this system.[24] Platforms should also deal with notifications without undue delay, efficiently and comprehensively, including removing or disabling the problematic offers and undertaking deterrent measures regarding the sellers behind these offers.[25]

Despite such initiatives, there has been a growing sense of dissatisfaction with the system based on the provisions of Articles 14 and 15 of the e-Commerce Directive, as it lacks effectiveness and concreteness in terms of applicable safeguards for the affected parties.[26] This dissatisfaction may be seen at the national and EU level and is reflected in two tendencies: on the one hand, to provide for more concrete rules on the notice-and-action procedure, including making certain elements obligatory and providing deadlines; on the other hand to demand increasing proactivity on the side of hosting service providers, culminating in the Commission Proposal for the Digital Services Act.[27]

An example of the first tendency at the national level is the recently enacted German Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) (*Netzwerkdurchsetzungsgesetz* – NetzDG),[28] targeting specifically hate speech and fake news.[29] This law provides for a compliance regime in respect of the notice-and-action procedure,[30] obliging operators of social networks to include a procedure for notification of illegal (according to the scope of the law) content and the law also provides deadlines for removal.[31] This procedure must be easy to spot, accessible and always available, the providers must immediately take notice of the complaint and examine it. Manifestly unlawful content must be taken down or blocked within 24 h from the moment of receiving the complaint; if the content is unlawful, but not manifestly so, this deadline is, in principle, 7 days. An alternative procedure is provided which allows the provider to transfer the decision regarding unlawfulness to a recognised self-regulation institution, the decision of which has to be accepted. Users and people submitting complaints must be informed about the follow-up of their complaints with reasons given.[32]

A similar law concerning combatting hate speech had been adopted in France, the so-called Loi Avia,[33] but has since been struck down by the French Constitutional Council.[34] The Law *pour la confiance dans l'économie numérique* 2004–575 of 21 June 2014[35] already contains a presumption of knowledge on the side of the provider if the particular elements provided for in the Law are furnished to the provider (Article 6 (5)).[36] Loi Avia was supposed to, inter alia, simplify the notifications element and to oblige the removal of certain illicit content within 24 h.[37]

[20] Katharina Kaesling, "Privatising Law Enforcement in Social Networks: A Comparative Model Analysis", (2018) *Erasmus Law Review* 151, 155.

[21] https://ec.europa.eu/newsroom/just/document.cfm?doc_id=42985.

[22] Ref Ares(2016)3934515- 26/07/2016. Available at: https://ec.europa.eu/docsroom/documents/34122/attachments/2/translations/en/renditions/native (hereafter: Memorandum of Understanding).

[23] Signatories of the Memorandum of Understanding (MoU) on the sale of counterfeit goods via the internet, available at: https://ec.europa.eu/docsroom/documents/34122/attachments/1/translations/en/renditions/native.

[24] Memorandum of Understanding, p 3.

[25] Ibid.

[26] See for instance: Aleksandra Kuczerawy, "From 'Notice and Takedown' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression", in Giancarlo Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press 2020.

[27] 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, COM/2020/825 final (hereafter: DSA).

[28] Netzwerkdurchsetzungsgesetz, available in English at: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=798A2B22B939C8AEEA23B03619CC3544.2_cid289?__blob=publicationFile&v = 2.

[29] Katharina Kaesling, "Privatising Law Enforcement in Social Networks: A Comparative Model Analysis", (2018) *Erasmus Law Review* 151, 155.

[30] Sandra Schmitz-Berndt, Christian M. Berndt, The German Act on Improving Law Enforcement on Social Networks: A Blunt Sword?, available at: https://ssrn.com/abstract=3306964, 16.

[31] Katharina Kaesling, "Privatising Law Enforcement in Social Networks: A Comparative Model Analysis", (2018) *Erasmus Law Review* 151, 156.

[32] Section 3 NetzDG.

[33] The final version, after most of its provisions have been struck down, is available here: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970. The version of the bill before the intervention of the Constitutional Council can be accessed here: http://www.assemblee-nationale.fr/dyn/15/textes/l15t0419_texte-adopte-seance.

[34] Conseil Constitutionnel, Décision n° 2020-801 DC du 18 juin 2020, https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm.

[35] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[36] Such elements include: details of the notifier, description of the problematic content and its location; reasons for withdrawing the content, including the legal provision declaring such content to be illegal, and copy of the correspondence with the author or editor requesting the taking of action or information why contact with the latter was impossible.

[37] http://www.assemblee-nationale.fr/15/propositions/pion1785.asp. On national provision in other MS, see European Commis-

In order to facilitate and intensify the implementation of good practices in the fight against illegal content, as well as to bring clarity regarding the protective framework and the position of providers, the EU Commission issued a Communication on Tackling Illegal Content Online.[38] According to the Communication: "Online platforms should put in place effective mechanisms to facilitate the submission of notices that are sufficiently precise and adequately substantiated to enable the platforms to take a swift and informed decision about the follow-up".[39] As to the platforms, they should remove illegal content as fast as possible.[40] The approach proposed in the Communication was further developed in the Recommendation, which includes rules on submitting notice, transparency, safeguards and protection against abuse. In particular, and in contrast to the Communication, it singles out terrorist content (anticipating in that sense the Terrorist Content Online Regulation – see below in this Section), and provides more stringent rules.[41]

The above instruments are either silent or contain broad and very general rules as to the protective framework for persons affected by these decisions, effectively leaving space to the providers for creating these procedures. The "Code of conduct on countering illegal hate speech online" requires the companies only to "have in place clear and effective processes to review notifications regarding illegal hate speech". The "Memorandum of Understanding on the sale of counterfeit goods via the internet" is similarly silent. Also, the NetzDG offers few possibilities for uploaders to contest the decision to take down the content uploaded by them.[42] A bill amending the NetzDG, currently in the German Bundestag, would add a provision regarding the review of decisions of the service providers, but only providing the basic elements of that procedure.[43] The Communication and the Recommendation are more vocal in that respect, providing rules on counter-notices against over-removal and abuse of the system (e.g. the possibility to contest a notice).[44] These rules are, however, quite broad, leaving many details still to be supplied by the service providers, upon which the effectiveness of these remedies will depend. It should also not be forgotten that the Communication and the Recommendation are not binding instruments.

At the same time, there is an increasing demand for proactivity in the analysed instruments. For instance, the Communication requests online platforms to adopt proactive measures. The paragraph states that providers should "adopt effective proactive measures to detect and remove illegal content online and not only limit themselves to reacting to notices which they receive. Moreover, for certain categories of illegal content, it may not be possible to fully achieve the aim of reducing the risk of serious harm without platforms taking such proactive measures".[45] The Communication links this instruction with the development and use of automatic technologies permitting detection and filtering of content, which are, to a certain extent, already in use.[46] The Recommendation goes in the same direction, while it also recognises the need for "effective and appropriate safeguards".[47] Proactive measures are also required in the "Memorandum of Understanding on the sale of counterfeit goods via the internet".[48]

A binding instrument, which exemplifies all the above-mentioned tendencies, is the recently adopted Regulation on addressing the dissemination of terrorist content online.[49] It is an instrument that goes even further in both of the directions mentioned above: obliging service providers to remove content, mandating a certain level of proactivity, while providing only a general obligation to ensure a protective framework.

It is worth having a look at the Commission's original proposal of that Regulation, in which these tendencies were even more apparent.[50] In that version the Regulation would have formulated expressly a duty of care: "Hosting service providers shall take appropriate, reasonable and proportionate actions in accordance with this Regulation, against the dissemination of terrorist content and to protect users from terrorist content".[51] The proposal formulated three categories of duties: removal orders, referrals and proactive measures. Removal orders were decisions requiring the hosting service provider to remove terrorist content or disable access to it, which need to be executed within one hour.[52] They were subject to sanctions in case of non-compliance.[53] A referral was a notice sent by a competent authority concerning content that might be considered to be of a terrorist nature.[54] The proposal did not provide for penalties for not removing the content. The

sion, *Overview of the legal framework of notice-and-action procedures in Member States SMART 2016/0039. Annexes to the Final Report*, July 2018.

[38] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms, Brussels, 28.9.2017 COM(2017) 555 final (hereafter: Communication).

[39] Communication, p 9-10

[40] Communication, p 13.

[41] Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online, C(2018) 1177 final, on terrorist content from point 29 (hereafter: Recommendation).

[42] Heidi Tworek, Paddy Leerssen, "An Analysis of Germany's NetzDG Law, Transatlantic Working Group", April 15, 2019, available at: https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf, p 8.

[43] See the proposed § 3b to be added to the NetzG, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes, Drucksache 19/18792, available at: https://dip21.bundestag.de/dip21/btd/19/187/1918792.pdf.

[44] Communication, p 16-17.

[45] Communication, p 10.

[46] Communication, p 12.

[47] Recommendation, point 18.

[48] Memorandum of Understanding, p. 5.

[49] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, hereafter: TERREG.

[50] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, 2018/0331 (COD) (hereafter: Regulation proposal). The Council adopted its General Approach in December 2018, available here: http://data.consilium.europa.eu/doc/document/ST-15336-2018-INIT/en/pdf. The position of the EU Parliament from 9.04.2019 is available here: https://www.europarl.europa.eu/doceo/document/A-8-2019-0193_EN.pdf.

[51] Article 3 Regulation proposal.

[52] Article 4 Regulation proposal.

[53] Article 18 (1) (b) Regulation proposal.

[54] Article 2 (8) Regulation proposal.

only duty subject to penalties would have been to assess, as a matter of priority, the content identified in the referral in the light of the providers' own terms and conditions and to take a decision on the removal or disabling of that content. The hosting provider would have to expeditiously inform the authorities about the decision taken. Furthermore, Article 6 of the proposed Regulation would impose the obligation on the service provider to take proactive measures in order to protect its services against the dissemination of terrorist content, i.e. uploading terrorist content as well as reuploading of the content previously removed or disabled as it was considered to be terrorist content.[55]

The adopted version of the Regulation does not formulate an express duty of care and no longer refers to proactive measures. Referrals have also been removed. However, even if it is less directly expressed, the role of service providers remains very proactive. A new Article 5 introduces so-called "specific measures", inspired by the earlier provisions regarding the duty of care and the proactive measures. This Article mandates service providers to include in their terms and conditions provisions addressing the misusing of their services for the dissemination of terrorist content online.[56] It also introduces a specific category of a hosting provider exposed to terrorist content, which arguably many big providers will easily fall within.[57] Such a provider should take specific measures to protect its services, but the choice of measures remains with the hosting service provider. While the Regulation offers some examples: "(a) appropriate technical and operational measures or capacities such as appropriate staffing or technical means", "(b) easily accessible and user-friendly mechanisms for users to report or flag to the hosting service provider alleged terrorist content", the real initiative rests with the service provider.[58] Service providers should also establish "an effective and accessible" complaints mechanism for people affected by the providers' decision to remove content.[59]

The above developments clearly show that there is an increasing expectation, translating into legal obligations as well, that service providers should take responsibility for controlling the content published on their services. At the same time, rules binding them in the carrying out of these tasks are limited, giving providers space for setting up rules and adjudicating in concrete cases.

It is also worth noting that the duties imposed on service providers might be problematic in view of the provisions of the e-Commerce Directive, for at least two reasons. The first reason is: does the application of proactive methods deprive the providers of the benefit of liability exemption offered by Article 14 of the e-Commerce Directive as it may lead to the obtaining of knowledge about the illicit aspect of the content in question?[60] The Commission considers that taking such voluntary, proactive measures does not automatically lead to the online platform losing the benefit of the liability exemption provided for in Article 14 of the e-Commerce Directive. The Commission's argument goes like this: firstly, the proactive monitoring does not amount to playing an active role in respect of individual content which removes safe harbour protection in accordance with *L'Oréal v eBay*.[61] Secondly, the fact that providers may acquire knowledge (actual or construed) may still be neutralised by removing or disabling the problematic content.[62] This reasoning has been criticised not only because it misses the difference in scale between stumbling upon illicit content and effectively looking for it, but also because it is not clear whether it provides liability exemption in the case of failing to identify illicit content.[63] A protection against such liability is offered for instance in the US legal system, a so-called Good Samaritan protection: Section 230 Communications Decency Act (CDA).[64] It is considered that the approach proposed by the Commission is more risky for the providers and should be recognised as such.[65]

The second reason is: there is also a controversy regarding the imposition of duty of care on service providers.[66] The e-Commerce Directive permits the Member States to require the application of a duty of care by service providers regarding the content which they store or might store.[67] The Communication suggests extending their obligation saying: "In addition to legal obligations derived from EU and national law and their 'duty of care', as part of their responsibilities, online platforms should ensure a safe online environment for users, hostile to criminal and other illegal exploitation, and which deters as well as prevents criminal and other infringing activities online".[68] However, it is not easy to distinguish the duty of care from a general monitoring obligation, which prompted some commentators to consider this duty to be in violation of the prohibition in Article 15 of the e-Commerce Directive.[69] It is

[55] Article 6 (1) Regulation proposal.
[56] Art. 5 (1) TERREG.
[57] Two final removal orders received by the provider within 12 months would be sufficient to put the provider into this category – Art. 5 (4) TERREG.
[58] Art. 5 (2) TERREG.
[59] Art. 10 TERREG.
[60] Aleksandra Kuczerawy, The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?, *CITIP Blog* 24 April 2018, https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5.
[61] CJEU, C-324/09 *L'Oréal v eBay*, ECLI:EU:C:2011:474.
[62] Communication, 11-12. The Recommendation repeats the conclusion and references of this reasoning in Recital (26) of the Preamble.
[63] Aleksandra Kuczerawy, The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?, *CITIP Blog* 24 April 2018, https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5.
[64] https://www.law.cornell.edu/uscode/text/47/230.
[65] Aleksandra Kuczerawy, The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?, *CITIP Blog* 24 April 2018, https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5.
[66] See for an analysis of the duty of care of intermediaries: Carsten Ullrich, Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective, (2017) 8 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 111.
[67] Recital 48 e-Commerce Directive. See also: Recommendation, 2.
[68] Communication, 7.
[69] Peggy Valcke, Aleksandra Kuczerawy, and Pieter-Jan Ombelet, *Chapter 6: Did the Romans Get It Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common*, in: M. Taddeo, L. Floridi (eds.),

worth noting that, while the original proposal of the Regulation against dissemination of terrorist content provided expressly for the duty of care, the final version not only does not contain it as such, but also states that the obligation under "specific measures" is to be without prejudice to Article 15 of the e-Commerce Directive.[70]

The most recent and, so far, most comprehensive effort to regulate the tasks of service providers in enforcement against illicit content has been the proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) submitted by the EU Commission on 15 December 2020.[71] The Digital Services Act (DSA) maintains the liability exemptions provided by the e-Commerce Directive as well as the prohibition on imposing general monitoring duties.[72] However, it provides for a comprehensive set of obligations on hosting service providers, especially on online platforms, with an even more enhanced set for very large online platforms. An online platform is defined in general as "a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information".[73] Online platforms become very large, if they "provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million".[74]

The DSA codifies – for all hosting providers of intermediary services – the notice-and-action procedures, providing in particular rules on how the mechanism should be offered to users, the elements of notice and the procedure for its treatment.[75] Online platforms are obliged to provide an effective internal complaint-handling system for decisions to remove or disable access to content or to suspend or terminate a recipient's account or the provision of the service to a recipient, as a result of the recipient's provision of content which is either illegal or incompatible with applicable terms and conditions.[76] The role of trusted flaggers is also codified with priority given to their notices.[77] Furthermore, platforms are obliged to suspend processing of notices and complaints coming from "individuals or entities or by complainants that frequently submit notices or complaints that are manifestly unfounded".[78]

As to the very large online platforms, one of the key additional obligations is the duty to analyse systemic risks regarding the concrete platform. These systemic risks include: the dissemination of illegal content; negative effects "for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child"; and intentional manipulation of the platform's services "with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security".[79] These platforms should provide for measures mitigating such identified risks.[80]

The DSA also provides for an enforcement system involving Member States and the Commission, the latter mainly as regards the very large online platforms. Competent authorities should have certain investigatory powers and the possibility to impose penalties and other measures.[81]

Even if the DSA is the most comprehensive Act so far produced as regards the framework of assessment of illicit content by service providers, it does not lower their need to take up an adjudicative role, but arguably confirms it. The DSA provides only very general criteria as to the application of restrictions by service providers: they should act in "a diligent, objective and proportionate manner",[82] and notices should be considered "in a timely, diligent and objective manner".[83] Restrictions might be a consequence of the provision of illegal content by recipients of service, but also a consequence of other infringements, defined in the terms of service by the provider. While the DSA would oblige platforms to provide a statement of reasons for decisions to apply a restriction (Art. 15 DSA) and access to an internal complaint-handling system (Art. 17 DSA), the description regarding the latter is again very general. It should be "easy to access, user-friendly and enable and facilitate the submission of sufficiently precise and adequately substantiated complaints".[84] Furthermore, complaints should be handled "in a timely, diligent and objective manner" and providers should reverse their decisions if there are "sufficient grounds" for it.[85]

By virtue of this system, the platforms' adjudicative role becomes effectively codified, while – commendably – put into a framework guaranteeing certain procedural rights. How far their power will reach depends also on the review available. According to Article 43, "[r]ecipients of the service shall have the right to lodge a complaint against providers of intermediary services alleging an infringement" of the DSA. It is hard to predict how far this Article – if it is kept in the final version of the Act – could be the basis for assessment of the above-mentioned broad criteria defining the standard that the providers should apply. A review mechanism may be also provided in national law.[86] It is also worth noting that, according to the DSA, recipients should be able to use services of out-of-court dispute settlement bodies, which should be impartial and independent of online platforms and certified by competent authorities in the Member States.[87]

"The Responsibilities of Online Service Providers", Springer 2017, 109-110.

[70] Art. 5 (8) TERREG.

[71] 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, COM/2020/825 final (hereafter: DSA)

[72] Art. 3-5 and 7 DSA.

[73] Art. 2 (h) DSA. An exception is made for services where dissemination is a minor and purely ancillary feature.

[74] Art. 25 (1) DSA.

[75] Art. 14-15 DSA.

[76] Art. 17 DSA.

[77] Art. 19 DSA.

[78] Art. 20 (2) DSA.

[79] Art. 26 (1) DSA.

[80] Art. 27 DSA.

[81] Art. 38-60 DSA.

[82] Art. 12 (2) DSA.

[83] Art. 14 (6) DSA.

[84] Art. 17 (2) DSA.

[85] Art. 17 (3) DSA.

[86] Recital 47 DSA.

[87] Art. 18 DSA.

3. Digital evidence

In December 2015 in a terrorist attack in San Bernardino, California, two attackers killed 14 people and later died in a shootout with the police. Following the attack, the FBI recovered a password-protected iPhone 5, belonging to one of the attackers. The FBI requested (by means of the All Writs Act) Apple to unlock the phone. It effectively meant compelling Apple to write new software that would let the government bypass the security of such devices and unlock the phone. Apple refused to do so because of its policy not to undermine the security of its products, even under the threat of legal action.[88] The company preferred to stick to the principle, which is important for their business model, and send a message to their clients that it will keep promises in terms of privacy protection even under threat of sanctions.[89] However, the court indefinitely suspended the proceedings as the FBI managed to access the data with the help of professional hackers. Their services cost $900,000 and the FBI did not find any information not previously known to the investigators.[90]

This case is very revealing as to the frustration of law enforcement authorities when accessing digital evidence, the key role of service providers in obtaining this access as well as their role as adjudicators as to conflicting values at stake.[91]

It is not only cybercrime, but also virtually any type of offence which might potentially leave a digital trace, which might serve as evidence in criminal procedure. Therefore, access to this data – which is in possession of ISPs – is not only attractive for law enforcement, but becomes crucial given how much of human activity occurs digitally nowadays. National criminal procedure laws provide for rules allowing the authorities to access data, while protecting suspects' procedural safeguards. However, very often the service provider in question is foreign or the data in question is held on a server located in a different country. In such cases instruments of cross-border cooperation need to be used, either the ones provided within the EU, in particular the European Investigation Order (EIO), or mutual legal assistance (MLA) outside the EU.

A number of technical and legal difficulties are linked with this framework. Amongst the practical difficulties, the most important ones are: limited possibilities of enforcement, encryption, lack of data and loss of location. Law enforcement authorities attempting to access data from an unwilling provider may coerce the provider by imposing fines and hoping that they will be sufficiently compelling. A classic tool of criminal procedure, such as a search and seizure of servers, will have limited utility, while being extremely disruptive for the functioning of the business in question. In order to find the required data, law enforcement authorities would need to apply disproportionate resources. This problem is further exacerbated if – and this is often the case – data is encrypted. Additionally, it might be that the ISP does not store the data at all, if communication is done peer-to-peer.

The problem of loss of location is particularly relevant in this context. The increasing use of cloud technology, for instance by Google, results in "sharding" data into numerous small pieces stored in different locations.[92] For this reason, it is virtually impossible to determine the location of data, and thus it is also unclear as to which law and authorities of which country or countries are applicable and competent.[93] In response to this and the above problems, some states, such as Russia and China, imposed mandatory data localisation within their territory as regards data of their citizens, with negative consequences for Internet infrastructure and the openness of the net.[94]

The discussion on e-evidence started before the entry into force of the EIO, when the legal framework was less practical for law enforcement.[95] Yet, even the EIO has been criticised for being too slow and cumbersome for the digital era, in particular by the Commission,[96] although this criticism is not uniformly shared.[97] Much less practical, in any case, are

[88] Leander Kahney, "The FBI Wanted a Back Door to the iPhone. Tim Cook Said No", *Wired* 16.04.2019, accessible at: https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/. "In the matter of the search of an Apple iPhone seized…" Order of 16 February 2016 compelling Apple, Inc. to assist agents in search, No. ED 15-0451 M, accessible here: https://assets.documentcloud.org/documents/2714005/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf.

[89] Tim Cook, "A Message to Our Customers", 16 February 2016, available at: https://www.apple.com/customer-letter/.

[90] Leander Kahney, "The FBI Wanted a Back Door to the iPhone. Tim Cook Said No", *Wired* 16.04.2019, accessible at: https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/.

[91] Interested readers may also see the reflections of the author on the topic of the gathering of digital evidence: *All evidence is equal, but electronic evidence is more equal than any other. The relationship between the European Investigation Order and the European Production Order*, (2020) 11 NJECL Issue 2, available at: https://journals.sagepub.com/doi/full/10.1177/2032284420919802; *Mutual recognition by private actors in criminal justice? Service providers as gatekeepers of data and human rights obligations*, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517878.

[92] Vivek Krishnamurthy, "Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters", Berkman Klein Center Research Publication No. 2016-3 (February 18, 2016), https://ssrn.com/abstract=2733350.

[93] On technical and legal difficulties in gathering digital evidence, see also: Katalin Ligeti, Gavin Robinson, "Transnational Enforcement of Production Orders for Electronic Evidence. Beyond Mutual Recognition?", in: R Kert, A Lehner (eds), *Vielfalt des Strafrechts im internationalen Kontext: Festschrift für Frank Höpfel zum 65. Geburtstag* (NWV 2018) 628-632.

[94] Internet Society, "Internet Way of Networking Use Case: Data Localization", published on 30 September 2020, available at: https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/

[95] See on the shortcomings of the EIO in that context: Anonymous 2020, Details omitted for blind reviewing.

[96] Commission Staff Working Document, Impact Assessment, Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' (Brussels, 17.4.2018 SWD (2018) 118 final) 23.

[97] See for instance the report of the CEPS and QMUL Task Force, "Cross-border data access in criminal proceedings and the future of digital justice. Navigating the current legal framework and exploring ways forward within the EU and across the

the MLA procedures, which are particularly burdensome, requiring the involvement of diplomatic channels and lasting around one year.[98] Given the fact that the most important providers are American, MLA is of great importance as it is the default procedure as regards cooperation with the US. On the requesting side it imposes the formulation of the request in a way which permits the American authorities to prove the existence of probable cause (that the evidence gathered will prove the offence). As it is a legal concept not known in Europe, many prosecutors or judges formulating requests might not provide sufficient elements to attain this threshold. The US Department of Justice – on its side – needs to engage resources into checking and litigating the request, while there is no particular American interest involved beside the fortuitous fact of the use of an American service.

Because of these shortcomings, there is a clear frustration of law enforcement, especially in truly local cases, where perpetrators, victims and location of the crime remain within one country, while only the service used turns the case into a cross-border one. This frustration resulted in a number of developments aimed at remedying the situation, the result of which is the significant involvement of service providers in deciding whether to grant access to the data or not.

In the first place, law enforcement authorities resorted increasingly to voluntary cooperation of service providers.[99] The applicability of that form of cooperation depends on the lack of prohibition on such cooperation in the law applicable to the service providers and on the willingness of the service providers to cooperate. As the cooperation is not compulsory, there is no guarantee that service providers would actually provide the requested data. Cooperation with foreign law enforcement authorities might be forbidden, as is the case for content data in the US.[100] However, non-content data may be transferred by US providers to non-US law enforcement authorities voluntarily. As there is no concrete legal framework for this type of cooperation, it is for the service providers to set up rules on how to assess requests coming from foreign law enforcement authorities and how to react to them.[101] This method is also devoid of a protective framework for the people concerned; hence it leaves in the hands of the ISPs the decisions on cooperation and assessment of legality or proportionality of requests.[102] These types of assessments are typical for public bodies but not for private actors.

A more compelling way of dealing with the problem was the unilateral imposition of duties in a cross-border context, with the prominent example of Belgium. Requests for data are, in principle, governed by the principle of territoriality. Belgium famously abandoned this in the case against Yahoo, claiming that the foreign provider cannot protect itself from the local obligations if the link with Belgium can be established, because the provider offers services targeting Belgian citizens (taking into account the domain name, languages of the service and targeted advertising).[103] This approach – upheld by the courts and later codified in the Belgian Code of Criminal Procedure – is particularly inconvenient for service providers, if the law applicable according to classic territoriality forbids the production of data in the case in question (which was the case for Yahoo).[104]

In the face of shortcomings and limitations of voluntary cooperation and the difficulties created by unilateral imposition of duties, the need for a framework has become clear, resulting in initiatives on both sides of the Atlantic. Thus the US amended the law forbidding US providers to transfer content data to foreign law enforcement authorities by enacting the CLOUD Act of March 2018. The transfer will be allowed, however, only after an agreement is reached between the US and the country in question, which permits such transfers, and which is based on the assessment of the rule of law and standards of privacy protection.[105] So far only one such agreement has been signed, with the UK,[106] while the agreement with Australia is still being negotiated.[107] The possibilities that the CLOUD Act offers will also have a significant impact on requests coming from the EU, including a potential agreement of the same kind, which is also linked with the e-evidence proposal.

The Commission issued the so-called e-evidence proposal, which aims at facilitating the cross-border exchange of digital evidence within the EU. It is composed of two instruments: a regulation and a directive. The Directive would mainly serve to guarantee effective enforcement, by requiring the Member States to ensure that service providers offering services in the

Atlantic", available at: https://www.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf, pp. 12-16.

[98] Statement of Jennifer Daskal to the Committee on the Judiciary Subcommittee on Crime and Terrorism United States Senate. Hearing on Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights, May 10, 2017.

[99] EU Commission Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, 3.

[100] 18 U.S.C. §§ 2702. See: Jennifer Daskal, "Unpacking the CLOUD Act", (2018) 4 *eucrim*, 220.

[101] See for instance for Google: https://policies.google.com/terms/information-requests.

[102] Europol, SIRIUS EU Digital Evidence Situation. Report 2019. Cross-border access to electronic evidence, 20 December 2019, available at: https://www.europol.europa.eu/sites/default/files/documents/sirius_eu_digital_evidence_report.pdf.

[103] Vanessa Franssen, "The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?" (2017) 3 Eur. Data Prot. L. Rev., 534, 538ff.

[104] An analogous case concerned Skype, with a similar conflict with Luxembourgish law. See on that: Vanessa Franssen, Marine Corhay, "La fin de la saga Skype: les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger", 2019 *Revue de Droit Commercial Belge* 1014-1022.

[105] Jennifer Daskal, "Unpacking the CLOUD Act", (2018) 4 *eucrim*, 220, 222-223.

[106] Theodore Christakis, 21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts), published on 17 October 2019 at: www.europeanlawblog.eu. See also: Marcin Rojszczak, "CLOUD act agreements from an EU perspective", (2020) 38 Computer Law & Security Review.

[107] Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton, 7 October 2019, available at: https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

European Union have to designate a legal representative in the EU empowered to receive and respond to the orders described in the Regulation.

The key element of this proposal is the Regulation (EPOR), which, if adopted, would introduce two new instruments: a European Production Order and a European Preservation Order. A European Production Order (EPO) is issued by a judicial authority in one Member State and compels a service provider in another Member State to produce electronic evidence.[108] A European Preservation Order is a similar order but requesting preservation of electronic evidence in view of a subsequent request for production.[109] This analysis will focus on the Production Orders as they are more problematic from the point of view of fundamental rights and choices which ISPs have to make.

A number of key features of this proposal are meant to address shortcomings of other forms of cooperation. Firstly, it would create an EU-wide system of acquiring data by law enforcement authorities through the direct cooperation of service providers, which would involve the authorities of the state of the provider (called "the enforcing state") only in a case of non-cooperation. Secondly, the system would not be based on territoriality linked to the place where the data is stored. As it is a common framework for the Area of Freedom, Security and Justice, the conflicting legal obligations within this area will be avoided. Thirdly, the deadlines for producing data are short, much shorter than for the EIO (10 days since the reception of the order in normal circumstances, and 6 h in urgent cases).

While the focus of the EPOR is European, it plays an important role for the exchange of data with the US. Beforehand, it had been unclear whether the US would negotiate with the EU as an entity or with each Member State separately. The EPOR "Europeanised" the matter. The Commission received in 2019 the mandate to enter negotiations with the US.[110] As mentioned above, content data cannot at present be voluntarily disclosed by US service providers to EU law enforcement authorities, while the service providers may be obliged to do so by virtue of the law of some Member States. Once signed, this agreement will allow the avoidance of these conflicting obligations for US providers and permit the latter's adherence to the duties stemming from national or EU law.[111]

As to the state of the legislative process, the Council issued its General Approach at the end of 2018,[112] and the report of the EU Parliament was issued in December 2020.[113] The trilogue negotiations are expected to begin very soon. The initiative has been criticised from almost every angle and it is beyond the scope of this article to summarise this criticism. The following analysis will focus on a number of key elements demonstrating the position of the ISPs and their relationship with law enforcement authorities. The analysis will first consider the original draft presented by the Commission, pointing out where necessary the changes proposed by the Council. The approach of the EU Parliament differs more significantly from the original proposal than does the Council's version, so it will be addressed subsequently. The alterations which the EU Parliament proposed do not – arguably – change the main proposition of this article as to the role of private actors.

According to Article 7 of the draft Regulation the EPO "shall be addressed directly to a legal representative designated by the service provider for the purpose of gathering evidence in criminal proceedings". The ISP is supposed, in principle, to produce the respective data. The EPOR recognises that, for a number of rather practical reasons, e.g. incompleteness of the order or its manifest errors, the ISP may not be able to produce the requested data. The service provider must seek clarification and, if possible, preserve the data in the meantime.[114] If the service provider is in a situation of de facto impossibility of producing the data, and this situation was not self-inflicted, it should lead to the withdrawal of the order.[115] In a case where the ISP does not comply with the entirety of the order for other reasons, it must also explain such reasons to the issuing authority and the authority must take into account any new information while reviewing the order.[116]

In a case of non-cooperation by the ISP, the engagement of a competent authority in the state where the order is addressed (enforcing authority) may be triggered, which transforms the order into a more classic mutual recognition instrument, similar to the EIO. The grounds for refusal are more limited in comparison to the latter and concern mostly the validity of the issuance of the decision and the possibility of complying with it. Two of the conditions for issuing the order cannot be verified at this stage, however, namely whether the measure is available in the issuing state and whether the order is necessary and proportionate. Questions of the impact on fundamental interests of the enforcing state (such as national security and defence) and related to privileges and immunities may also be invoked. The General Approach of the Council suggests introducing a ground of refusal linked with the determination and limitation of criminal liability relating to the freedom of the press and freedom of expression. There is also no consen-

[108] Art. 2 (1) EPOR.

[109] Art. 2 (2) EPOR. A European Production Order may be issued so that a European Preservation Order can be issued later, but could also be followed by a mutual legal assistance request or a European Investigation Order: Art. 6 (2) EPOR.

[110] Recommendation of 5.02.2019 for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM (2019) 70 final. The Council took the positive decision on 21 May 2019, Doc. 9114/19.

[111] However, such conflicts may still exist with other countries, if a provider falling within the scope of the EPOR is compelled to provide data in the EU. The EPOR addresses this problem, but the details of the clause are still under discussion. In particular, it is under consideration whether the EU authorities will always be allowed to persist with the order, even if it puts the ISP in legal jeopardy. Arts. 15-16 EPOR in the original proposal and the General Approach of the Council and Article 14a of the Parliament position.

[112] Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - general approach, 2018/0108(COD).

[113] The position of the EU Parliament is available here: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.pdf (hereafter: EPOR-Parliament).

[114] Art. 9 (3) and (6) of the draft Regulation.

[115] Art. 9 (4) of the draft Regulation. The version of the Council struck out the sentence that expressly said it. However, another outcome would be hard to justify.

[116] Art. 9 (5) EPOR.

sus yet as to the presence of a fundamental rights ground for refusal.

According to the EU Commission proposal (and the Council's General Approach) the ISPs may play a role in the invocation of refusal grounds, but only to a limited extent. The ISP may oppose the order because of reasons related to the conditions of issuing the order (if it was not issued or validated by the competent authority, issued for offences to which it was not applicable or the service is not covered by the Regulation), because the order contains manifest errors, or because of the factual impossibility (de facto impossibility or the order does not concern data stored by or on behalf of the service provider at the time of receipt of the order). The original proposal would allow the ISPs to invoke fundamental rights concerns in a case of manifest violations of the Charter or manifest abuse, which is denied in the General Approach. Unlike the enforcing authorities, ISPs cannot invoke fundamental interests of the enforcing state, reasons related to privileges and immunities or to the freedom of the press or freedom of expression.

Non-compliance will be punished with sanctions to be provided by the Member States. The Council added a clause expecting the Member States to ensure the possibility of imposing a sanction of up to 2% of the total worldwide annual turnover, which in that version could theoretically already have been used for the first infringement.[117]

The possibilities for service providers to question the orders are limited. According to the philosophy of the proposal, the ISP is the provider of data and should do it without questioning the legitimacy of the order. It is also theoretically shielded from the order's legal deficiencies. Recital 46 of the proposal states that "[s]ervice providers should not be held liable in Member States for prejudice to their users or third parties exclusively resulting from good faith compliance with an EPOC or an EPOC-PR".[118] However, despite this statement giving them such a limited role, ISPs will not be able to abstain from verifying the validity of requests and may find themselves in situations where questioning the order will be necessary, even under the threat of fines, similar to the situation in the Apple-FBI dispute.

According to that proposal, ISPs would necessarily be the first filter of requests. They would play the role which, in the classic mutual recognition setting (e.g. European Arrest Warrant), is played by the executing authority. One can imagine a number of potential scenarios when their position might come into conflict with the issuing authority. For example, they might receive requests to provide data for offences which are not criminalised in the state where they operate and where public opinion does not accept the criminalisation of such acts. The pressure from NGOs, public opinion, politicians, and even from the government may add to ISPs' reluctance to comply. Another problem might arise from requests coming from Member States which are not up to the standard of the rule of law, making it possible for the Article 7 TFEU procedure to be opened against them. Requests may be problematic as they may concern issues dividing public opinion. For instance, some see the leaders of the Catalan independence movement as criminals, while others support them. An ISP may have users from both factions and will be compelled to side with one of them if requested to produce data on these people. State interests might also be involved and stronger ties to a certain government's interests might influence ISPs' choices. These are decisions which are public in nature, and they will have to be taken under a threat of sanctions.[119] They might not deter the ISPs from non-compliance, however, as was exemplified by the FBI-Apple dispute. How effective these threats are is another issue, as their imposition and enforcement would potentially require litigating with economic behemoths.

The proposal for the EPO in the Parliament's version addresses some of the problems mentioned above, applying a specific variable geometry and attempting to limit the privatisation of enforcement. In particular, it introduces an obligatory notification of the state where the order is addressed.[120] As regards "subscriber data and IP addresses for the sole purpose of identifying a person", service providers should transmit the requested data as soon as possible.[121] However, the competent authorities of that state may invoke one of the refusal grounds compelling the receiving authorities to erase data thus obtained or blocking the transfer, if it has not yet occurred.[122] In that sense the notification does not have a suspensive effect, whereas it does have such an effect concerning traffic and content data. For these types of data, service providers should not execute the order before the time has elapsed for the competent authorities of that state to refuse the EPO.[123] Furthermore, as to the "issuing State [...] subject to a procedure referred to in Article 7(1) or 7(2) of the Treaty on European Union", the service provider cannot transmit the requested data until it receives explicit written approval from the competent authority in the state where the order is addressed.[124] Finally, the list of grounds for refusal is broader than in both the original proposal and in the Council's General Approach, and can be read even as including the possibility of questioning the necessity and proportionality of the order.[125] The possibilities for service providers to invoke the grounds for refusal remain very limited and the final decision on the execution of the order belongs to the competent authorities.[126] However, it is worth noting that this version revives the possibility for service providers to question the order

[117] Art. 13 EPOR. A similar provision (although amounting to 4% of the hosting service provider's global turnover of the last business year) is provided for in the draft Regulation on preventing the dissemination of terrorist content online, Art. 18 (4), but it requires a systematic failure to comply.

[118] This is the formulation from the Council's General Approach. The Commission's formulation was less straightforward, but in the same vein. The version proposed in the Report of the Parliament transfers this rule to the text of the Regulation: Art. 13 (1a) without, however, limiting the scope of the rule to "good faith compliance".

[119] A more extensive analysis of this argument can be found here: Anonymous 2020, Details omitted for blind reviewing.

[120] Art. 7 (1) (b), 8a (1) and 9 (1a), (10) (1a), EPOR-Parliament.

[121] 8a (2) EPOR-Parliament.

[122] 8a (4) EPOR-Parliament.

[123] 9 (2b) EPOR-Parliament.

[124] 9 (2a) EPOR-Parliament.

[125] 10a, in particular 10a (1) EPOR-Parliament.

[126] 14(3) EPOR-Parliament.

on the grounds of it being "manifestly abusive or [...] exceeding [its] purpose".[127]

It remains to be seen what shape the final version of the EPOR will take. The idea of introducing the e-evidence initiative was mainly to alleviate the regime in order to facilitate the exchange of data without burdening the authorities of the Member State of the provider with analysing potentially numerous requests. Even if the final version of the EPOR contains the obligatory notification of the state of the provider, it does not guarantee that all (or a majority) of orders will be verified by the competent authorities. Even the EU Parliament's approach does not include a formal obligation to do so (except for requests for traffic or content data issued by states subject to Article 7 TFEU procedure).[128] In that case the main filter will again be the service provider.

It is inevitable that digital evidence will play an ever-increasing role in criminal procedure, which is a direct consequence of the role which technology plays in everyday life. Regardless of the final design of the EPOR, and including voluntary cooperation and in particular cooperation with the US service providers, service providers will continue to play a significant role in the access to data, assessing whether to comply with orders or to refuse to do so. In controversial cases, as the FBI-Apple dispute demonstrates, they will not hesitate to refuse to comply based on their own assessment of validity and proportionality of requests.

4. From compliance duties to enforcement and adjudication

The above analysis shows that service providers – private actors – play a very active – proactive – role in enforcement and are compelled to perform acts of balancing rights and values against each other in a way that assimilates their role to the adjudicative role of public actors.

The idea of involving private actors in regulation and enforcement is not new as such. In past years we have observed how private actors have been increasingly engaged in regulation and enforcement. This engagement could either take the form of co-regulation or self-regulation or of purely private regulation and enforcement. For some while, regulation and enforcement have not been the monopoly of the state. This phenomenon is reflected by theories such as responsive regulation or smart regulation.[129]

In addition, the private sector has been frequently co-opted in the fight against crime. David Garland coined the term "responsibilization strategy", to depict this new role of the private sector that focuses heavily on crime prevention.[130] Examples include anti-money laundering strategies or the duty to gather and later transmit certain data to the authorities, like telecommunications data, taxation data or passenger name records.

Today, however, we are clearly moving beyond smart regulation and beyond "responsibilization" of the private sector in regulation and enforcement. Private actors do not only take part in designing rules for their sector but they are the ones responsible for defining infringements. Private actors do not simply assist public enforcement by implementing rules; today private actors proactively counter infringements and design strategies and tools to do so. They are required to proactively assume these roles, either because the proactivity is mandated (the Terrorist Content Online Regulation and the Digital Services Act), effectively encouraged (Recommendation on illegal content) or results from a practical necessity of service providers (content moderation in view of services' policies and electronic evidence). Private actors also occupy this space under their own initiative as the Facebook Oversight Board exemplifies.[131] In addition, private actors perform value judgments, balancing conflicting rights against each other. In the extreme, this may lead to even disobeying state orders and giving preference to the protection of certain values based on a business judgement, as shown by the FBI-Apple example.[132]

This pushes the service providers more towards the public sphere, constituting a true paradigm shift. In general, businesses are not supposed to make value judgments, as this is left to the public sphere. A good example of this philosophy is the debate over conscientious objection or other types of objections which allow people to refuse to serve other people for different moral reasons.[133] Even where this is accepted, it remains an exception (requiring legal grounds), demonstrating that the balancing of fundamental rights is a function of public authorities.

In this new setting, private actors may be compelled to balance such potentially conflicting rights as: the freedom of expression, the rights to respect for private life, the freedom to conduct a business, the rights of the child, the rights

[127] 10(6) EPOR-Parliament.

[128] In particular the reading a contrario of Art. 9 (2a) EPOR-Parliament shows the lack of obligation to verify every request outside the hypotheses of this article.

[129] Madeleine de Cock Buning, Linda Senden, Introduction: EU Private Regulation and Enforcement Mapping its Contextual, Conceptual, Constitutional and Citizens' Dimensions, in: Madeleine de Cock Buning, Linda Senden, Private Regulation and Enforcement in the EU, Hart Publishing 2020.

[130] David Garland, "The Limits of the Sovereign State - Strategies of Crime Control in Comtemporary Society" (1996) 36 Brit J Crim 445, 452-455.

[131] On intermediaries as 'private judges' see also: Diane Rowland, Uta Kohl, Andrew Charlesworth, *Information Technology Law*, Routledge 2016, Chapter 3: Intermediary Liability, 73, 85-87; Georgios N. Yannopoulos, "The Immunity of Internet Intermediaries Reconsidered?", in: M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer 2017, 31.

[132] Another example may constitue the conflict between the Indian Government and Twitter, in which the former requested the latter to delete or desactivate numerous accounts in the context of protests against the new agriculture laws. Twitter refused to comply with some orders regarding journalists and activistits claiming that the request violates Indian law. Statement of Twitter "Updates on our response to blocking orders from the Indian Government" of 10 February 2021 is available at: https://blog.twitter.com/en_in/topics/company/2020/twitters-response-indian-government.html.

[133] See for instance the case of a refusal to produce a wedding cake for a homosexual couple: *Masterpiece Cakeshop v. Colorado Civil Rights Commission*, 584 U.S. ___ (2018).

to protection of (intellectual) property and the right to non-discrimination.[134]

However, performing this function fundamentally clashes with the very nature of private actors, which are profit-orientated entities. They may act for a greater good or even have a benefactor or do-gooder profile, but a public policy cannot rely on it as private actors may behave in such a way only as long as it is beneficial for them.[135] This business logic is well exemplified by the FBI-Apple encryption dispute, where Apple gave priority to its reputation for protecting clients' privacy over the needs of an investigation in a terrorist case.[136] Whereas exercising the public function of adjudication would presuppose impartiality and independence, private platforms are guided by their business model that is geared towards profit generation. Such considerations are, however, alien to the public domain. The recent investigations launched against Amazon well expose this conflict of interest: the EU Commission launched an investigation against Amazon for antitrust violations for using information acquired as a platform in order to compete as a seller of similar products.[137]

While ISPs will have to make choices between conflicting values in a similar way to public actors, unlike the latter, ISPs may have to perform their role facing the risk of sanctions of a different nature and other disadvantageous consequences including, for instance, reputational ones. In such cases, businesses will have to decide according to their business interests.

Moreover, the problem of the business logic guiding private actors is linked with the problem of accountability and responsibility. The value judgments that belong to the public sphere are linked to a democratic system of accountability,[138] but companies are foremost accountable to their owners.

The transfer of "public" power also creates risks specific to abuses of that power. For instance, employees may be made the subject of corruption proposals concerning decisions where the stakes are high. What is the real nature of such corruption: is it private or is it more assimilated to the public arena? A person commits corruption in a private sphere if he or she breaches the duty towards the entity for which he or she works.[139] In the situations discussed here, it is not necessarily the duty towards one's own company but, in a way, towards society, hence assimilating it to the nature of public corruption.

5. Factors reinforcing the trend

The problem with this new role of private actors is becoming even more pertinent as a number of factors point not only towards the perpetuation of this trend, but even towards the likelihood of its aggravation. These factors can be grouped into three categories: 1) nature of digital technology; 2) global nature of the Internet; and 3) current state of digital capitalism.

1). *Nature of digital technology*

The primary material of digital technology is data, a combination of 1 s and 0 s. Data has a huge replication capacity, hence allowing for easy spread of content, incomparable to technologies available beforehand. Two factors are crucial in this respect: scale and time. Data can be replicated and spread across the Internet or become accessible from anywhere, easily reaching large numbers of people. This can happen in practically no time. These two factors – scale and time – also create significant problems for law enforcement authorities, which often respond too late and insufficiently due to an inadequate legal framework, limited resources or lack of technological capacities. In that sense, service providers may be quicker and react on a larger scale as they are the ones controlling the data.

At the same time, the amassing of immense amounts of data creates an unprecedented opportunity for law enforcement. Never in the history of the world has so much information been accumulated, including about people's private lives and their criminal intentions or activities. Well performed research may reveal even more about us than we know ourselves.[140] Human memory is imperfect, while the storage of data is relatively cheap and being undertaken on a vast scale. Data treated by sophisticated analytical tools may reveal information about human behaviour on a larger scale (big data) and about individuals in particular, thereby helping to prevent or investigate crime.

This data is gathered by service providers; the essence of digital capitalism is the gathering of data.[141] The interest of law enforcement authorities to have access to these possibilities is obvious, but it requires the cooperation of the holder of such data, namely the ISPs. At the same time, technology creates significant limitations for law enforcement. One of the key problems is the location of data which can create legal difficulties for law enforcement authorities which are seeking access to data (see Point 2, below). The need for the cooperation of the ISPs also results from technological inaccessibility. If an ISP refused to produce data, traditional tools of law enforcement, such as a dawn raid on a data centre, would be

[134] Recommendation, 3-4.

[135] Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech", (2018) 131 Harvard Law Review 1598, 1627.

[136] In a similar vein see: Diane Rowland, Uta Kohl, Andrew Charlesworth, *Information Technology Law*, Routledge 2016, Chapter 3: Intermediary Liability, 73-125, 123.

[137] Commission Decision of 17.07.2019 to initiate antitrust proceedings in case AT.40462 Amazon Marketplace Amazon, press release available at: https://ec.europa.eu/competition/antitrust/cases/dec_docs/40462/40462_6210_9.pdf.

[138] On accountability and its assessment, see in particular: Mark Bovens, "Public Accountability", in: Ewan Ferlie, Laurence E. Lynn Jr., and Christopher Pollitt (eds.), The Oxford Handbook of Public Management, OUP 2007.

[139] Articles 1 and 2 of the Council Framework Decision 2003/568/JHA of 22 July 2003 on combating corruption in the private sector, OJ L 192/54.

[140] Bruce Schneier, *Data and Goliath*, W. Norton & Company 2015, 26.

[141] Shoshana Zuboff, The Age of Surveillance Capitalism, in particular 8-12 (What is Surveillance Capitalism?).

useless as the authorities would encounter significant difficulties in locating the necessary data, except by means of disproportionate resources. Additionally, increasingly often it is difficult to even locate the data, given the technology employed in cloud computing (loss of location).[142] Encryption adds another layer of complexity.[143] Fines remain the only possibility to compel a provider to provide the required data, while their compelling power might be limited in view of the financial resources at the disposal of the digital behemoths.

2). *Global nature of the internet*

It is at the same time, however, an obvious but not wholly true statement that the Internet has no borders. It is true, however, as regards countries that do not impose significant Internet restrictions. These borders are easily crossed by digital content and services are accessible across borders. For instance, it is difficult, if not practically impossible, to prevent, on a global scale, content from appearing on the Internet. The difficulty in enforcing the right to be forgotten beyond the borders of a particular jurisdiction was recently demonstrated in the ECJ judgement in *Google v CNIL*.[144]

At the same time, borders create a significant obstacle for law enforcement authorities which, in principle, cannot cross them.[145] This presents a particular challenge as law enforcement authorities either need to use instruments of international cooperation or unilaterally claim jurisdiction in order to compel service providers to comply with their orders. Both options create the sorts of problems already discussed in this article. For this reason direct involvement of service providers is being sought as a solution.[146]

The global nature of the Internet also presents a challenge for service providers engaged in policing their area of operation. Perceptions as to conflicting values differ, as do legal frameworks in many aspects, even within the EU. These discrepancies may put service providers in conflicting situations. The multinational way of functioning results in the fact that service providers operate the same service in countries with different cultures and different sets of values.[147] For instance, if a conservatively leaning country makes a request that reflects an approach which is considered to be unacceptable in a much more liberal country, e.g. regarding criminalisation of abortion or blasphemy, service providers will have to consider whether to fulfil the request at the risk of alienating liberal clients or refuse it at the risk of sanctions and potential backlash from conservative clients. A similar dilemma might arise regarding the problem of the Catalan independence movement, which divides Spain and which has led to the conviction of Catalan politicians, some of whom escaped, e.g. to Belgium. If asked, should an ISP provide data on such a politician, or refuse claiming that he or she is persecuted for political reasons? In these types of cases, the problem may be exacerbated by the pressure from NGOs and media. While conflicts and polarisation increase, value judgments are being transferred to private actors. How should they make these judgments given the diversity of their clients (which include private persons, companies and governments)? In other words, if a duty of care is being imposed on the ISPs, they might be confronted with the question: according to which values should this duty of care be tailored? As they are private actors, their ultimate guide is business interest which does not have to be aligned with the general public interest.

In terms of content moderation, the offer is often tailored depending on the country of access. However, countries can be internally torn between factions displaying heated animosity which puts significant pressure on service providers. The conflicts in the US concerning the most recent presidential election are a good case in point. The decision of platforms to suspend the accounts of President Trump after the attack on the US Capitol has been praised by some, and can be understood in view of the need to stop any incitement to violence. However, the decision has been subject to critical reaction not only from the partisans of Donald Trump, but also inter alia by the German Chancellor, Angela Merkel and the European Commissioner for Internal Market, Thierry Breton, for demonstrating the excessive power which lies in the hands of service providers.[148]

This debate is also part of the reflection on digital sovereignty. One aspect of it is the sovereignty of states vis-à-vis service providers and the other is the push, in particular

---

[142] Jennifer Daskal, "The Un-Territoriality of Data", (2015) 125 *Yale Law Journal* 326, 365-375.

[143] Also, some providers might use technology depriving them from access to users' data in order to avoid liability, e.g. Apple. On encryption and enforcement, see: Orin S. Kerr, Bruce Schneier, "Encryption Workarounds", (2018) 106 *Georgetown Law Journal* 989.

[144] CJEU, Case C–507/17, *Google v CNIL*, ECLI:EU:C:2019:772. See for an analysis of this judgment: Cedric Ryngaert and Mistale Taylor, "Implementing the right to erasure: the judgment of the EU Court of Justice in Google v CNIL", posted on 8 October 2019 at: http://blog.renforce.eu. On the other hand, for a discussion on the so-called "Balkanisation" of the Internet which is taking place and which concerns the question of the cross-border nature of cyberspace, see: "Debate: We Need to Protect Strong National Borders On The Internet. Debate Between Jennifer Daskal and Paul Ohm, moderated by Pierre De Vries", (2018) 17 Colorado Technology Law Journal 13.

[145] S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7). In the context of cyberspace, see Ulrich Sieber, Carl-Wendelin Neubert, Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty, (2017) 20 Max Planck Yearbook of United Nations Law Online 239.

[146] Another solution is to agree on some common rules for tolerated encroachments into territory, such as those provided in the Budapest Convention (Art. 32) and proposed in its Second Additional Protocol, currently under negotiation. However, the scope of application of Art 32 is limited as, it seems, will be the scope of the Second Additional Protocol (see the version of 10 November 2020 available here: https://rm.coe.int/provisional-text-of-provisions-2nd-protocol/1680a0522c). Another solution pursued so far on a theoretical level is reconceptualization of the concept of territoriality, see e.g.: Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle*, Oxford University Press 2017.

[147] Services may be tailored to regions, but this tailoring not only gives power to service providers, but also subjects them to potential criticism.

[148] Pierre-Paul Bermingham, Merkel among EU leaders questioning Twitter's Trump ban, 11.01.2021, available at: https://www.politico.eu/article/angela-merkel-european-leaders-question-twitter-donald-trump-ban/

by the EU, to impose rules as to the services concerning EU citizens.[149]

3). *Current state of digital capitalism*

Another key factor is the way in which the digital market has evolved, with some ISPs having become essential channels of communication. Key providers, such as Google or Facebook, not only offer the most popular services, but have been acquiring other popular services (e.g. YouTube and Instagram) thereby increasing their dominance.[150] This creates a situation of quasi-monopoly, similar to the way in which states have a monopoly on deciding on certain issues within their "territories".[151]

In view of this dominance, the impact of the decisions of these ISPs can be extremely significant. The example of an influencer is pertinent here. If his or her account, which is followed by millions of users, is deactivated, e.g. by Instagram due to illicit content, it may de facto close down a business. Part of the business model is to be present at one of the most popular platforms, hence the possibilities of switching to another platform are limited. A ban impacts the influencer in question as well as his or her staff and other stakeholders, as well as potentially causing a loss of tax revenue. A service provider might deliver a death sentence to a business, potentially without the adequate safeguards which would normally be required if this were done by public authorities. In addition, illicit content cannot be identified as such in all cases without controversy. It is the same for a manufacturer whose main place of activity is Amazon Marketplace, if he or she is banned from the service for allegedly offering counterfeit goods. At the same time, there is a clear risk of discrimination by service providers in such circumstances.

The size in terms of users of the main providers makes them indispensable for many individuals and business entities, thereby further strengthening the power of these technological behemoths. This makes them also indispensable for law enforcement authorities, to help them police the providers' vast "territories", even taking over the law enforcement authorities' tasks. The size in economic terms also makes these companies formidable enemies in potential litigation. To all of this should also be added that dominant service providers are often at the forefront of technological innovation either through their own development or by acquisition, with legislation and law enforcement usually lagging behind in that respect.

[149] Luciano Floridi, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, (2020) 33 *Philosophy & Technology* 369.

[150] Google owns YouTube, Facebook owns Instagram and WhatsApp, Microsoft owns LinkedIn.

[151] Mark Zuckerberg: "In a lot of ways Facebook is more like a government than a traditional company. We have this large community of people, and more than other technology companies we're really setting policies." David Kirkpatrick, *The Facebook Effect: The Inside Story of The Company That Is Connecting The World*, Simon & Schuster 2010, 254, cited from: Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech", (2018) 131 Harvard Law Review 1598, 1599. See also Anupam Chander, "Facebookistan", (2012) 90 N.C. L. Rev. 1807.

6. Need for rethinking the role of private actors

The above analysis demonstrates how, in certain areas, the role of private actors in enforcement has become much more like the function normally associated with public authorities. The analysis also demonstrated that the current legal framework is not adapted to this new situation. Solutions are being sought in concrete areas, but with insufficient results and such solutions are far from being comprehensive. At the same time, the factors analysed above point to the increasing necessity for cooperation with private actors in law enforcement, including them playing this "public" role. Unless there is a significant change in the design of technology and the nature of digital capitalism, the phenomena described above will only intensify.

For these reasons, there is a need for a deep rethinking of the status of private actors, in particular ISPs, in the process of law enforcement and their relationship with the responsible authorities. On a broader scale, this reflection should also learn from and contribute to the larger discussion on the role of businesses in society and on the governance of cyberspace.

In order to proceed with this rethinking, two questions are crucial. 1) How much can and should private actors be guardians of fundamental rights? 2) How can fairness be guaranteed in the proceedings in which private actors play this public role?

As to the first question, it is embedded in the problem of how much the state must have the monopoly on every aspect of law enforcement and how much it can "outsource" to private parties. The role the financial (and other) institutions play in combatting money laundering and financing of terrorism is a good example showing that many aspects of enforcement are shared between public and private bodies. The idea that private actors may be directly bound to safeguard fundamental rights is already present in the jurisprudence of the ECtHR under the horizontal effect or *Drittwirkung*.[152] Yet, the level at which service providers are confronted with issues regarding fundamental rights is much higher than the hypotheses in the ECtHR case law. We are not talking anymore about not violating another private party's fundamental rights, but about actively solving conflicts regarding these rights. Hence, besides "shared enforcement", we can speak of "shared adjudication". There is a need for a through reflection whether such "shared adjudication" should be allowed and, if so, what its boundaries should be.

Furthermore, the existence of "shared adjudication" means that there is a need to provide fairness in these proceedings, which leads to the second crucial question. This concern has also already been recognised in some of the instruments regarding content moderation, although with little consequence

[152] On the application of fundamental rights in private law (horizontal effect or *Drittwirkung*), see in particular: Olha Cherednychenko, *Fundamental Rights, Contract Law and the Protection of the Weaker Party: a Comparative Analysis of the Constitutionalisation of Contract Law, with Emphasis on Risky Financial Transactions*, Sellier European Law Publishers 2007, in particular chapter 4. Dean Spielmann, Companies in the Strasbourg courtroom, C.J.I.C.L. 2016, 5(3), 404-417. See also: Recommendation, 3.

in terms of tackling the problem, while the proposal for the Regulation regarding electronic evidence does not seem to address the issue sufficiently, as demonstrated above. The law should either prevent service providers from playing the "public" role, but if it cannot, or, as we can observe, if it *de iure* or *de facto* pushes them to do that, it should also provide a framework assuring that rights of affected persons can be sufficiently safeguarded and that they are not at the mercy of the providers guided necessarily by their business interests. That question is linked with a broader issue of accountability. While there are established mechanisms of accountability of public bodies, this novel setting requires novel concepts, which would provide sufficient controls according to standards of democratic societies. A good example of addressing the deficit of accountability is the history of EU agencies, many of which have been reformed recently in order to increase control over them.[153] Yet, these agencies are still public bodies. A reflection on accountability in the context of private actors requires taking into account of their nature. Subjecting the duties of private actors to heavy penalties does not seem to be a sufficient and effective way of assuring such a control.

Even if it does not belong to the domain of enforcement as such, one more aspect needs to be taken into account. While solving the problems described above, the choices should also be informed by the need to create a fair digital market. Its current design is subject to significant criticism and numerous actors are under investigation, e.g. for anti-competitive practices.[154] The digital market is dominated by few players and heavy duties may create hurdles that will make it even less likely for new players to enter the market. This problem was to some extent recognised by the DSA, which creates significantly more duties for "very large" platforms.[155]

7. Concluding remarks

For years private actors have been subject to increasing duties. However, as far as service providers are concerned, their tasks are currently moving from compliance towards more proactive enforcement and they are also playing an adjudicative role, making them similar to public actors. This transformation results from a number of factors embedded in the technological and market setting of cyberspace and the digital economy. While law enforcement cannot avoid relying on private actors, they remain profit-driven entities and this creates significant conflicts of interest.

Unless there is a sudden and profound reversal of the trends described above, the need for private actors' participation will only increase. For instance, the development of the Internet of things, and its application for instance in city governance ("smart cities"),[156] intensifies the possibilities for law enforcement and the needs of policing.[157] The development of artificial intelligence will also contribute to this debate as it will place greater importance on the question: how much control can public – in particular judicial – authorities lose? Artificial intelligence is increasingly being used – not without controversy – for predictive policing and to make predictions for procedural measures. It is likely that private actors will remain better positioned to design the necessary technology. Yet, AI may be a self-taught black-box fed with data and the process of obtaining its results cannot be fully comprehended and explained.[158] AI has proved effective already, for instance for cancer predictions. However, one would worry less about the procedure being inexplicable in the case of a machine being able to correctly predict the risk of cancer. This is less so the case for the justice system where procedure is no less important than the correct outcome, as it is the case in criminal proceedings.[159] The impossibility of explaining the outcome of an algorithmic prediction and thus the resulting impossibility of questioning that measure may violate different procedural rights.[160] Nonetheless, the attractiveness of the ability to anticipate future crime and the potential for unbiased judgement that AI might offer is also hard to deny.

These examples show that the numbers of areas where the participation of private actors in law enforcement in such ways that they take over control of the process, are likely to be growing. Hence, a deep reflection on the framework of their participation in the execution of a public function is urgently needed. This reflection should not succumb to the regulatory pessimism which sometimes dominates the reflection on Internet governance. While certain aspects of the Internet's functions and its structures need to be taken as a given, this does not mean that regulatory influence is impossible.[161] Even while transferring part of its competences to private actors, law enforcement should not abandon efforts to enhance its own technological capacities. If private actors are to take over public functions, this should still remain a carefully regulated exception.

---

[153] Alex Brenninkmeijer, Miroslava Scholten (eds.), *Controlling EU Agencies: The Rule of Law in a Multi-jurisdictional Legal Order*, Edward Elgar Publishing, May 2020.

[154] Commission Decision of 27.6.2017 relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search (Shopping)), C(2017) 4444 final; Commission Decision of 17.07.2019 to initiate antitrust proceedings in case AT.40462 Amazon Marketplace Amazon, press release available at: https://ec.europa.eu/competition/antitrust/cases/dec_docs/40462/40462_6210_9.pdf.

[155] Art. 25 (1) DSA.

[156] Elizabeth E. Joh, Policing the smart city, (2019) 15 International Journal of Law in Context, 177.

[157] See: Eldar Haber, The Wiretapping of Things, (2019) 53 UC Davis Law Review 733.

[158] Claude Castelluccia and Daniel Le Métayer, Understanding algorithmic decision-making: Opportunities and challenges, 2019, EU Parliament Study, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf.

[159] There is a difference in approaches between in particular inquisitorial and adversarial systems in that respect, but even the former – which attaches more importance to the truth – does not neglect the procedure.

[160] Aleš Završnik, "Algorithmic justice: Algorithms and big data in criminal justice settings", 2019 European Journal of Criminology, available at: https://journals.sagepub.com/doi/full/10.1177/1477370819876762.

[161] Julie Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, OUP 2019, 1.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.