Article

The obligation to notify suspicions of criminal offences in the Digital Services Act under scrutiny

dr. A. (Anna) Pivaty & mr. dr. P.T.J. (Pieter) Wolters*

1. Introduction

More and more often, private actors become involved in criminal law enforcement. National governments and the EU increasingly seek to 'partner' with the private sector to ensure public security. Seeking public-private partnerships has become a popular law enforcement strategy with respect to certain types of crime, such as money laundering, corruption, organised crime, terrorism, as well as, more recently, cybercrime. Private actors are encouraged, or in certain cases mandated, to provide information to public law enforcement authorities to facilitate detection or investigation of such crimes. The assistance of private actors is enlisted because they possess a large amount of information necessary to uncover certain criminal activities, not readily accessible to public authorities.

Content moderation and combating illicit content online, where digital service providers play a crucial role, is another prominent recent example of private-public enforcement of criminal law.[1] Various obligations of digital service providers to inform law enforcement authorities already exist in national laws, e.g. in German law,[2] and in EU law under the Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online (hereinafter 'Terreg').[3] Besides these specific laws, the recently adopted Digital Services Act (hereinafter 'DSA') revises the European framework for the responsibilities of intermediary services (Section 3).[4] It also includes a new, broader obligation to report crimes of which digital service providers become aware. Pursuant to article 18 DSA, 'online platforms' and other 'hosting' services are obligated to inform law enforcement authorities about criminal offences 'involving a threat against life and safety'.

In this article, we question whether this new provision of DSA strikes a proper balance between the public interest of prosecuting such crimes and the infringement on fundamental rights such as freedom of expression and privacy. We draw inspiration from (debates around) various existing provisions on mandatory reporting of crime for digital service providers and other private actors in EU and certain domestic laws.

Section 2 discusses the existing mandatory reporting laws. Examples from EU and domestic jurisdictions are used to illustrate rationales for and risks inherent in

* Anna Pivaty is Assistant Professor Criminal Law at the Faculty of Law of Radboud University (Research Centre for State and Law; Research programme Conflict Resolution Institutions). Pieter Wolters is Associate Professor Private Law at the Faculty of Law of Radboud University (Radboud Business Law Institute; Interdisciplinary Hub for Digitalization and Society).

1 S. Tosza, 'Internet service providers as law enforcers and adjudicators. A public role of private actors,' *Computer Law & Security Review* 2021/43, p. 2 onwards.

2 Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, NetzDG), § 3a.

3 OJ L 172, 17.5.2021, p. 79-109.

4 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) PE/30/2022/REV/1, OJ L 277, 27.10.2022, p. 1-102.

doi: 10.5553/BSb/266669012022003005004

such legislation. Section 3 contains an analysis of article 18 DSA in view of findings in Section 2. In conclusion (Section 4), we argue that, although article 18 DSA seems to be grounded on clear rationales, it contains pitfalls and risks that must be further addressed.

2. Existing laws on mandatory reporting of criminal offences

The obligation of digital service providers to inform law enforcement authorities about criminal offences under DSA resembles the existing duties imposed under domestic and EU laws on private individuals and organisations to report certain types of criminal activity. In this Section, we argue that exposing the rationales for and concerns raised in respect of these provisions can be useful in the analysis of article 18 DSA. Section 2.1 first describes the various laws concerning reporting obligations of private actors in general. Section 2.2 subsequently zooms in on the (to our knowledge, limited) examples of laws that impose reporting obligations specifically on digital service providers.

2.1 Mandatory reporting laws in general

Traditionally, domestic criminal laws refrain from imposing a general obligation on private actors to report crime. In common law systems, the long-standing principle recognised in jurisprudence is that generally, a failure to inform police about an ongoing or committed criminal offence is not an offence in itself.[5] The rationale for this principle is that the opposite might result in a society where private actors are compelled to systematically spy on each other. Thus, crime reporting obligations of private actors should remain limited, and they should always be weighed against the public interest of prosecuting particular offences. This balancing exercise involves considerations not only of seriousness of the offence, but also effectiveness: namely, whether imposing the duty of private reporting will lead to more successful detections and ultimately convictions.[6]

A similar legal principle exists in continental law systems. For instance, under Dutch law the obligation of private actors to inform about ongoing or past criminal activity has been limited to most serious crimes.[7] Thus, article 160 of the Dutch Code of Criminal Procedure contains an obligation of individuals to report certain crimes to police, namely crimes against the state, crimes against life, human trafficking, rape and kidnapping. This obligation extends to inchoate crimes (i.e. the stages of 'preparation' or 'attempt,' both punishable by criminal law), but not to crimes that are only being planned. Generally, there is no sanction attached to this obligation, except for specific circumstances.[8] The rationale behind this provision is to assist authorities in detecting (very serious) crimes, which otherwise might not come to their attention.[9] Attempts to extend these mandatory reporting provisions were met with scepticism. Thus, recent research into the desirability to extend the obligation of mandatory reporting from rape to other sexual offences, following a legislative proposal in the Parliament,[10] concluded that a general reporting duty was of no added value.[11] Specifically with regard to mandatory reporting of child sexual abuse, it was argued that such provision was not necessary, because criminal prosecution is not always in the best interest of the child.[12]

Despite the traditional reluctance to extend private crime reporting obligations, recently there has been a surge of domestic laws imposing obligations to report (suspected) criminal activity by private actors. These laws vary greatly in terms of their subject matter, scope of the reporting obligations, persons who must report and authorities they should report to, as well as sanctions attached to non-compliance. The main rationale for these laws is similar to that behind the respective Dutch provisions: to increase referrals of certain crimes to law enforcement authorities. These are usually those crimes, which are relatively rarely reported to the authorities, and in respect of which the state has a particularly strong duty to intervene, for instance because the harm inflicted by those crimes is especially serious, or due to international obligations to prosecute such crimes (or both).[13] An extension of the duty of care, as shown in examples below, is another common rationale for mandatory reporting laws. Finally, political pressures are also likely to play a role in the adoption of these laws. Thus, anti-terrorist and anti-terrorist financing laws, which contain clauses on mandatory reporting, were adopted as a response to the 2001 Al-Qaeda attack in the US.[14] The German Network Enforcement

5 See e.g. in relation to US: M. Hall, 'An emerging duty to report criminal conduct: banks, money laundering, and the Suspicious Activity Report,' *Kentucky Law Journal* 1995/6, p. 743.

6 P. Bekker, 'A saga of snitches and whistleblowers: the boundaries of criminal liability for breach of statutorily-imposed duties especially in the context of organised crime,' in: J. Joubert (ed.), *Essays in Honour of CR Snyman*, Pretoria: University of South Africa 2008, p. 15-16.

7 R. Kool, F. Kristen, T. Beekhuis, and W. de Zanger, Verruiming van de aangifteplicht voor ernstige seksuele misdrijven?, Den Haag: WODC 2019, p. 61.

8 Where the crime in question has taken place, and where timely informing the police about it could have prevented it; or where the failure to inform about an already-committed crime led to serious harm to the health or life of the victim. See art. 136 Dutch Criminal Law Code.

9 Kool etal. 2019, p. 61.

10 Motie van het lid Groothuizen c.s. over verruiming van de aangifteplicht, *Kamerstukken II* 2017/18, 31015, nr. 142.

11 Kool et al. 2019, p. 15. See also for a critical assessment of the proposal, M. Groenhuijsen, 'Verruiming van de aangifteplicht voor zedendelicten: Is dat echt een goed idee?', *DD* 2019/5, p. 347-355.

12 See R. Kool, S. Kool, S. Kerssiers, and T. van der Rijst, 'Mind the (Knowledge) Gap: Towards a criminal duty to report child sexual abuse?,' *Utrecht Law Review* 2021/17, p. 33-45.

13 For instance, states have a duty to investigate and prosecute crimes against life and torture under so-called 'positive obligations' under arts 2 and 3 of the European Convention of Human Rights.

14 N. Ryder, 'Is It Time to Reform the Counter-terrorist Financing Reporting Obligations? On the EU and the UK System,' *German Law Journal* 2018/19, p. 1170.

doi: 10.5553/BSb/266669012022003005004

Act (hereinafter 'NetzDG') discussed below in Section 2.2 was adopted (and subsequently amended to include obligations of mandatory reporting) following concerns about proliferation of hate speech on social media as the result of a massive influx of refugees in 2015.[15]

A quick survey of domestic mandatory reporting laws reveals that they can be grouped into several themes. One example are laws imposing an obligation (usually) on caretakers to report abuse of vulnerable persons. For instance, several countries, beginning with the US in early 1960s, have enacted laws imposing duties to report child abuse.[16] These laws vary as to the subject of the duty (childcare professionals or all citizens), threshold for reporting, information that needs to be provided, and (criminal or civil law) penalties for failure to report. Other jurisdictions have introduced laws imposing obligations of caretakers to report abuse of elderly[17] or domestic abuse.[18] The rationale for the duty to report lies in the extension of the duty of care, as well as in the need to protect vulnerable populations from abuse that often occurs in private, and is rarely reported.[19]

The duty to report terrorist offences also appears rather common in domestic legal systems. One of the broadest obligations in this regard seems to be that found in South African law, where it is an offence punishable by a maximum sentence of five years' imprisonment for a person to fail to report to the police if they have reason to suspect that another person intends to commit a terrorism offence or has committed a terrorism offence or if they are aware of the location of a person who is suspected of intending or having committed such an offence.[20] This provision was criticised for its vagueness and its excessively broad scope.[21] Laws in other jurisdictions seem to be significantly narrower. In Canada, for instance, only failure to report property which a person knows to be owned by a terrorist is punishable, although with the maximum sentence of 10 years' imprisonment, which is rather high.[22] The duty to report terrorist offences seems to rest on the rationale of their imminent danger for life and safety of many persons. However, it has also been criticised due to the vagueness of the definition of terrorism, and the resulting risk of interference with the freedom of expression,[23] as well as, in the Canadian example, with the right to property (Section 7 Canadian Charter of Rights and Freedoms) due to its excessive breadth.[24]

The duty of banks, financial institutions and legal service providers to report suspicious transactions is another common type of a duty to report crime, imposed under national money laundering laws.[25] Similar provision were enacted by the EU, namely the four Anti-Money Laundering Directives, which require banks, financial institutions, and other persons such as lawyers or notaries, to monitor and report certain types of financial transactions to national anti-money laundering authorities (but not directly to law enforcement authorities).[26] Arguably, the rationales behind these provisions (whose reach is steadily increasing) are not entirely coherent and clear;[27] however the general assumption behind the duty to report suspicious financial transactions is that it helps to detect and combat other crimes than money laundering, e.g. terrorism and organised crime (which in turn attract much political attention). Yet, the effectiveness of these measures is continuously questioned.[28] Research has also shown that service providers tend to excessively and uselessly report to avoid heavy fines.[29]

In England and Wales, for instance, the effectiveness of the law, which requires service providers to report 'information that comes to them in the course of their business if they know, or suspect or have reasonable grounds for knowing or suspecting, that a person is engaged in, or attempting, money laundering or terrorist financing' (under the sanction of 14 months' imprisonment) is commonly questioned. Its possible ineffective-

15 W. Echikson and O. Knodt, *Germany's NetzDG: A key test for combatting online hate*, CEPS 2018, p. 14.

16 B. Mathews and M. Kenny, 'Mandatory Reporting Legislation in the United States, Canada, and Australia: A Cross-Jurisdictional Review of Key Features, Differences, and Issue,' *Child Maltreatment* 2008/13, p. 50-63.

17 See e.g. in respect to the US: Stetson Law University, *Mandatory reporting statutes for elder abuse* 2016, www.stetson.edu/law/academics/elder/home/media/Mandatory-reporting-Statutes-for-elder-abuse-2016.pdf concluding that all US states have some form of mandatory reporting of elderly abuse.

18 See e.g. C.E. Jordan and A.J. Pritchard, 'Mandatory Reporting of Domestic Violence: What Do Abuse Survivors Think and What Variables Influence Those Opinions?,' *Journal of Interpersonal Violence* 2021/36, p. 7-8 stating that in various US states there are laws on mandatory reporting of injuries associated with crime or due to use of certain weapons, abuse of children, abuse of vulnerable adults, and reporting of domestic violence.

19 Jordan and Pritchard 2021.

20 See Protection of Constitutional Democracy against Terrorist and Related Activities Bill 2003, Section 12(2).

21 Bekker 2008, p. 15.

22 S 83.1 Bill C-36, the Anti-terrorism Act 2001.

23 Bekker 2008, p. 15-16.

24 K. Roach, 'Canada's New Anti-Terrorism Law,' *Singapore Journal of Legal Studies* 2002, p. 137.

25 M. Hall, 'An Emerging Duty to Report Criminal Conduct: Banks, Money Laundering, and the Suspicious Activity Report Note,' *Kentucky Law Journal* 1996/84, p. 643-684. Under Dutch law, this is regulated via *Wet melding ongebruikelijke transacties*, which implements EU Anti-Money Laundering Directives.

26 For a comprehensive analysis of EU anti-money laundering legislation, see V. Mitsilegas and N. Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law,' *Maastricht Journal of European and Comparative Law* 2016/23, p. 261-293.

27 D.L. White, 'The Anti-Money Laundering Complex in the Modern Era,' *The Banking Law Journal* 2016/133, p. 1-59.

28 A recent comparative study finds for instance that 'the anti-money laundering policy intervention has less than 0.1 percent impact on criminal finances, compliance costs exceed recovered criminal funds more than a hundred times over, and banks, taxpayers and ordinary citizens are penalized more than criminal enterprises.' See R.F. Pol, 'Anti-money laundering: The world's least effective policy experiment? Together, we can fix it,' *Policy Design and Practice* 2020/3, p. 73-94.

29 E. Takáts, 'A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement,' *The Journal of Law, Economics, and Organization* 2011/27, p. 32-78; L. Della Pellegrina, G. Di Maio, D. Masciandaro, and M. Saraceno, 'Are Bankers "Crying Wolf"? The Risk-Based Approach in Money Laundering Regulation and its Effects,' *Italian Economic Journal* 2022, DOI: 10.1007/s40797-022-00195-2.

ness is attributed to the vagueness of the respective law, namely its failure to define 'any suspicious activity', which resulted in a low reporting threshold and consequently, an overflooding of the respective database with reports, most of which are not being investigated.[30]

In contrast, in Sweden, another reporting obligation with regard to financial crime exists, addressed at auditors, who must report certain criminal offences which they come across when undertaking audits to public prosecutors.[31] The law is drafted narrowly to include only specific types of offences, and only corporations (and not individuals) as potential perpetrators; and to provide only civil and not criminal liability for failure to comply with the obligation. This legislation was found (moderately) effective, largely thanks to its relatively targeted nature.[32] Besides their questionable effectiveness, criticisms of the duty to report suspicious financial transactions voiced in the literature revolve around the possible inroads into the clients' right to privacy due to the sweeping nature of obligations to report, and the fact that only a small portion of reports relates to criminal activity.[33]

2.2 Duties of digital service providers to report crime

With the global spread of the internet, the rates and proportion of crimes committed with the use of the internet, as compared to crimes not involving ICT, have increased.[34] These crimes, however, are generally more difficult for law enforcement authorities to detect due to lower reporting rates[35] and other hurdles to effective investigations.[36] As digital service providers possess valuable information about such crimes, laws were devised to mandate them to report certain crimes to public authorities. Although these laws are targeted (focusing on digital service providers only), they still present risks of encroachment upon fundamental rights (as discussed below), because of large amounts of information that is available online.

Until now, mandatory reporting provisions addressed at digital service providers have been scarce. Probably the first mandatory reporting laws, aimed at hosting providers and online platforms, were those adopted in Canada and the US, which concerned online child pornography. These laws were enacted following growing concerns about the spread of child pornography on the internet and the difficulties in obtaining information about publishers of such information.[37] In the US, the relevant law was adopted in 2008.[38] Under this law, electronic communication service providers which obtain information about a crime involving child pornography, must provide to a relevant child protection authority (CyberTipline of the National Centre for Missing Children) certain specific information enabling the identification of the alleged perpetrator(s); after which the latter authority might report to the relevant law enforcement agencies.[39] In Canada, under the law of 2011, persons providing internet service must inform the Canadian Centre for Child Protection when they 'have reasonable grounds to believe that child pornography is being or has been committed using their Internet service' (e.g. after being notified by a member of the public or an agency) by providing information specified in the respective law.[40] Similarly to the US approach, the child protection services will then notify law enforcement agencies in certain situations. Thus, these provisions differ from some mandatory reporting laws in that notifications are not made directly to law enforcement authorities, but to an (independent) intermediary. The rationale behind this is to strike a balance between the need for criminal prosecution, and the interests of the children involved, such as respect for their privacy and autonomy.

Another example of mandatory reporting laws addressed at digital service providers are the provisions in the (amended) German NetzDG. NetzDG contains provisions which mandate online platforms to take measures against content, which falls under the definition of hate speech crimes (22 offences in total) under German criminal law. An amendment to NetzDG, which entered into force on 3 April 2021, states that online platforms must, in addition, proactively report this potentially criminal content to the federal police. Non-compliance with this obligation leads to 'administrative' fines up to 50 million euros. The NetzDG, which gives additional force to combating a broad range of hate speech offences, was criticised for the risk of encroachment upon fundamental rights of users (freedom of expression), should alleg-

30 S.D. Norton, 'Suspicion of money laundering reporting obligations: Auditor compliance, or sceptical failure to engage?,' *Critical Perspectives on Accounting* 2018/50, p. 56-66.

31 B. Larsson, 'Patrolling the corporation – the auditors' duty to report crime in Sweden,' *International Journal of the Sociology of Law* 2005/33, p. 53-70.

32 Larsson 2005.

33 Other criticisms relate to the negative impacts on the trust relationship between the respective service providers and their clients. Mitsilegas and Vavoula 2016; Hall 1996; K.S. Helgesson and U. Mörth, 'Client privilege, compliance and the rule of law: Swedish lawyers and money laundering prevention,' *Crime, Law and Social Change* 2018/69, p. 227-248.

34 M. Tcherni, A. Davies, G. Lopes, and A. Lizotte, 'The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?' *Justice Quarterly* 2016/33, p. 890-911, Ch. 5; M. Akkermans, R. Kloosterman, E. Moons, C. Reep & M. Tummers-van der Aa, *Veiligheidsmonitor 2021*, CBS 2022, www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021.

35 Research shows that crimes with a digital element, even more serious ones, such as threat of violence, are less likely to be reported to police than traditional crimes. A. Graham, T.C. Kullig, and F.T. Cullen, 'Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice,' *Policing: An International Journal* 2021/43, p. 1-16.

36 See e.g. C.A.J. van den Eeden, J.J. van Berkel, C.C. Lankhaar, and C.J. de Poot, *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*, WODC 2021, p. 84-92.

37 See e.g. in relation to Canada: Legislative Summary, Bill C-22, Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, No. 40-3-C22-E (2010), p. 3; Office of the Federal Ombudsman for Victims of Crime, *Every Image – Every Child* 2009, p. 22-24.

38 The PROTECT Our Children Act of 13 October 2008.

39 18 USC 2258A: Reporting requirements of providers; Title 18 ('Criminal Procedure') US Code.

40 Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service (S.C. 2011); S. 11, Internet Child Pornography Reporting Regulations, SOR/2011-292.

doi: 10.5553/BSb/266669012022003005004

edly illegal content be overpoliced by platforms.[41] Additionally, the new amendment of NetzDG on mandatory reporting was subject to specific criticisms. Twitter, Google and other large platforms had recently instituted proceedings before the Cologne Administrative Court to challenge their duty to report crimes under German NetGZ, arguing *inter alia* that this obligation breaches the right to privacy of their clients due to the sweeping nature of the obligation to provide information, and requesting the Court to grant an injunction against this obligation.[42] Such an injunction was granted, although on different grounds, namely that requesting platforms established outside of Germany to provide such information is in breach of the E-Commerce Directive.[43]

On the EU level, the only piece of EU legislation next to DSA imposing a specific obligation on providers of digital services to report crime to law enforcement authorities is the Terreg.[44] The Regulation states in article 14(5) that hosting service providers[45] must 'promptly inform competent law enforcement authorities in the relevant member state or Europol, when they become aware of terrorist content involving an imminent threat to life'. The original Commission proposal read (then in art. 13(4)) that law enforcement authorities should be informed 'when hosting service providers become aware of any evidence of terrorist offences'. This was subsequently narrowed down to 'terrorist content involving an imminent threat to life'. Possible penalties for the breach of obligations under Terreg are defined under article 18, which states that member states should impose penalties, which are 'effective, proportionate and dissuasive' and that 'a systematic or persistent failure to comply' with the relevant obligations should be subject to penalties up to 4% of the hosting service provider's global annual revenue.

Recital 31 further specifies that 'to ensure proportionality, this obligation is limited to terrorist offences as defined in article 3(1) of Directive (EU) 2017/541' and that is 'does not imply an obligation on hosting service providers to actively seek any such evidence'. The Terreg is a rather controversial piece of legislation, which was criticised by academics and civil society organisations.[46] However, the criticisms related not so much specifically to article 14(5), but more generally to the various obligations of hosting service providers to detect and remove presumably terrorist content introduced by the Regulation, which would allegedly interfere with the freedom of expression. It was argued that the definition of terrorism was vague, causing risks of content expressing legitimate political protest being labelled as 'terrorist', particularly where automatic searches based on certain (combination of) words are used to detect it.[47] Many of these criticisms arise in the context of the specific offence of terrorism, which is particularly vague and controversial, and thus creates obvious tension with the freedom of expression. At the same time, the vagueness in the definition of the offence(s) to be reported obviously has a bearing on the clarity and effectiveness of the corresponding reporting provision.

2.3 Intermediary conclusion: rationales and risks of laws on mandatory reporting

As demonstrated in the preceding section, the number of mandatory obligations to report criminal activity is increasing, despite the existence of a general legal principle that private actors should not be forced to report crimes. This reflects the broader global trend of vesting private parties with duties to assist, sometimes proactively, in the enforcement of criminal law.[48] A more recent trend is the emergence of mandatory reporting laws addressed specifically at digital service providers.

The mandatory reporting laws rest on several rationales, namely the interest of better law enforcement (where the alleged crimes are particularly difficult for state authorities to detect, as in the case of money laundering or sexual offences), preventing serious and imminent harm (as in the case of duty to report terrorism or other life-threatening offences), and the extension of the duty of care (reporting obligations of caregivers). Reporting laws addressed at digital service providers mostly rest on similar rationales.[49]

However, laws on mandatory reporting of crime by private actors are often subject to controversy. First, many of the respective provisions are criticised for being excessively broad, due to broad definitions of the to-be-reported offences and of factual thresholds triggering the reporting duty. Second, some of the examined mandatory reporting laws (namely, on reporting terrorism and hate speech) – including those addressed at digital ser-

41 Although early research has shown that this risk did not seem to materialise, as platforms appeared reluctant to implement their new obligations, this low level of implementation raises doubts about effectiveness of NetzDG. See Echikson and Knodt 2018.

42 'Twitter files lawsuit against German online reporting rule', *Reuters* 21 January 2022, www.euronews.com/next/2022/01/31/twitter-files-a-lawsuit-in-germany-against-new-rules-on-reporting-or-blocking-criminal-con; 'Big tech opposes Germany's enhanced hate speech law,' *Euractiv* 1 February 2022, www.euractiv.com/section/internet-governance/news/german-reinforcement-of-hate-speech-law-faces-opposition-from-big-online-platforms/.

43 Art. 3(2) which requires that digital service providers should act in accordance with the laws of the Member States where they are established. See 'Germany: Administrative Court of Cologne Grants Google and Facebook Interim Relief; Holds Network Enforcement Act Partially Violates EU Law,' *US Library of Congress* 2022, www.loc.gov/item/global-legal-monitor/2022-03-30/germany-administrative-court-of-cologne-grants-google-and-facebook-interim-relief-holds-network-enforcement-act-partially-violates-eu-law/.

44 With the transposition deadline of 7 June 2022.

45 A provider of services, consisting of the storage of digital information provided by and at the request of a content provider. Art. 2(1) Terreg.

46 J. van Hoboken, *The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications*, Vrije Universiteit Brussels and University of Amsterdam 2019; Joint Open Letter Against Terreg of 75 European NGOs, 25 April 2020, https://edri.org/wp-content/uploads/2021/04/MEP_TERREG_Letter_EN_78.pdf; W. Bellaert, V. Selimi, and R. Gouwy, 'The end of terrorist content online?,' *Revue Internationale de Droit Penal* 2021/92, p. 163-187.

47 Bellaert et al. 2021.

48 See e.g. Tosza 2021.

49 The rationale of the extension of the duty of care does not appear to apply to digital service providers.

vice providers – potentially raise tension with fundamental rights, such as freedom of expression and right to privacy. Third, the effectiveness and proportionality of mandatory reporting laws is being debated (which is also in part related to their scope and relationship with fundamental rights). For instance, it is not clear whether mandatory, as opposed to voluntary reporting, and/or reporting to police, as opposed to other bodies independent from the state, is always necessary to achieve the stated goals. Related to this, punitive sanctions (e.g. criminal sanctions or large fines) are unlikely to be proportionate with regard to those mandatory reporting laws, the effectiveness of which is unproven, and to those which are potentially in tension with fundamental rights.

Generally, it seems accepted that laws imposing crime reporting duties on private parties should be subject to stringent requirements, namely the requirement of clarity and foreseeability (as citizens must know what is expected from them, especially if non-compliance is subject to penalties), as well as effectiveness or fitness-for-purpose, which in EU law is additionally reflected in the principle of proportionality.[50] This principle implies that the measure should pursue a legitimate aim, and be suitable and necessary to achieve this aim, as well as reasonable in view of legitimate interests of the persons affected by it.

3. The Digital Services Act and its article 18

The DSA revises the European framework for the liability and responsibilities of 'intermediary services' such as 'online platforms' and other 'hosting' services.[51] It is designed 'to contribute to the proper functioning of the internal market for intermediary services by setting out rules for a safe, predictable and trusted online environment'.[52] This includes the prevention of the dissemination of criminal and other forms of 'illegal content',[53] but also the facilitation of innovation and the protection of fundamental rights. The DSA therefore combines the protection of victims of illegal content, fundamental rights and economic interests.[54]

The core of the legal framework remains the same. Like the e-Commerce Directive, the DSA holds that these service providers cannot be held liable for transmitting or storing 'illegal content' that is provided by the 'recipients of the service'.[55] However, 'hosting' service providers can be held liable if they know about the illegal content and do not act expeditiously to remove or disable access to the information.[56] At the same time, the DSA also introduces new obligations for the providers of intermediary services,[57] including an obligation to report suspicions of criminal offences.

Pursuant to article 18 DSA, hosting service providers must 'promptly inform' criminal law enforcement authorities if they 'become aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place' and 'provide all relevant information available'. Recital 42b adds detail concerning the scope of this obligation and the reporting procedure.

In article 21 of the original Commission proposal, this obligation did not apply to all hosting service providers, but only to a specific subset: the online platforms. Online platforms do not just store the information, they also disseminate it to a potentially unlimited number of third parties. By extending the obligation to all hosting service providers, it now also exists for cloud computing or web hosting services.[58]

The possible penalties for non-compliance with these obligations is high. Pursuant to article 42(3), member states must ensure that the maximum amount of fines that may be imposed shall be 6% of the annual worldwide turnover of the hosting service provider in the preceding financial year.

This Section further examines article 18 DSA in view of the requirements to mandatory reporting laws formulated in Section 2.3, namely as to their rationale(s), scope, compliance with fundamental rights, effectiveness, and proportionality of sanctions.

(a) Rationale

Although the rationale for this specific DSA provision has not been specified in the *travaux preparatoires*, it seems to be grounded on the need to prevent imminent harm to life or safety of persons. Indeed, the clause describing the type of to-be-reported crimes generally reflects this rationale.

50 Craig and De Burca 2011, p. 526. See above with regard to Terreg.
51 DSA compromise, arts 1(1)(a), 2(f), (h).
52 DSA compromise, art. 1(1).
53 DSA compromise, art. 2(g).
54 For a more detailed description, see Raphaël Gellert and Pieter Wolters, *The revision of the European framework for the liability and responsibilities of hosting service providers* (Report for the Dutch Ministry of Economic Affairs and Climate Policy 2021). p. 14-18.
55 DSA compromise, arts 2(b), 3-5; e-Commerce Directive, arts 12-14.
56 DSA compromise, arts 2(f), 5(1)(a), (b); 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 [2000] OJ L178/1, art. 14(1)(a), (b). See DSA compromise, arts 2(f), 3-4; e-Commerce Directive, arts 12-13 about the conditions under which providers of 'mere conduit' and 'caching' services can be held liable.
57 See also DSA compromise, art. 1(1)(b).
58 DSA compromise, art. 2(h), (i), Recitals 13, 14. See also P.T.J. Wolters, 'De vlucht naar voren in de Digital Services Act', *AA* 2022/3, p. 195 about the distinction between online platforms and other hosting services.

doi: 10.5553/BSb/266669012022003005004

(b) Scope

Although article 18 seems to be grounded in a clear rationale, its scope appears too vague in several aspects, particularly when compared to the analogous provisions in domestic laws, as well as the Terreg provisions. First, it is not entirely clear which types of offences should be reported by service providers. The current text mentions 'criminal offences involving a threat to the life or safety of persons' (the original Commission proposal additionally referred to 'serious' offences). Although Recital 42b gives some examples of such offences, namely child sexual abuse, terrorism and human trafficking, it is unclear which other offences would fall under this category. Clearly, certain traditional offences such as murder, manslaughter or kidnapping would qualify, provided that information about such offences is published online. It is however less evident whether and under which conditions, for instance, online threats or some forms of hate speech would also be subject to the reporting duty. A general obligation to report hate speech in particular needs to be carefully assessed in view of the right of freedom of expression.[59] It is also unclear whether child pornography would fall under the reporting obligation, due to its close relationship to child sexual abuse.[60]

Furthermore, service providers are required to provide information which gives rise to a 'suspicion' of criminal activity. It is not further clarified what type or level of suspicion is required to trigger reporting. Criminal law knows, for instance, different gradations of 'suspicion,' such as 'reasonable suspicion' (the lowest gradation) or 'serious suspicion'. As discussed in the section above, a similar provision in English law was criticised for its vagueness and for establishing an excessively low threshold, which led to over-reporting. Under DSA, for instance, a low threshold for a suspicion might lead to reporting potentially innocent content, such as journalistic, artistic or academic expression being interpreted as glorification of violence or incitement to terrorism.

Next, the question arises when a hosting service provider should be considered 'aware' of the (risk of a) criminal offence and thus has an obligation to report. A similar issue exists in relation to the civil liability for hosting illegal content.[61] A hosting service provider can only be held liable if it has 'actual knowledge' or is 'aware' of the illegal content pursuant to article 5(1) DSA. In general, the provider cannot be considered to have actual knowledge of all content that is hosted through its services. It can only be held liable if it has knowledge about *specific* illegal content.[62] A hosting service provider can obtain this knowledge through its own investigations.[63] However, it cannot be obligated to do so as article 7 DSA prohibits general monitoring obligations. Similarly, the circumstance that a provider carries out voluntary investigations on its own initiative does not cause it to be liable for any illegal content that it may have missed pursuant to article 6 DSA. In this light, actual knowledge is mostly obtained through notices. Pursuant to articles 14(2) and (3), sufficiently precise and adequately substantiated notices give rise to actual knowledge if they allow a diligent provider of hosting services to identify the illegality of the content without a detailed legal examination. Although not stated explicitly, it seems reasonable to apply the same norms to 'awareness' in the context of article 18. This interpretation also provides some measure of clarity by limiting the reporting obligation to situations in which the provider has specific knowledge and to content that is clearly illegal.

Lastly, the relevant DSA provision also covers offences that are likely to take place, i.e. offences that are only being planned or prepared. It is unclear how and based on which criteria service providers are expected to establish that the 'offence is likely to take place'. This may cause hosting service providers to be overcautious and start reporting too many threats. Thus, the requirement to report on offences that are 'likely to take place' might be both excessively vague, as well as impracticable and thus ineffective. The wording such as an 'imminent threat' of an offence taking place, similar to the clause in US law on child pornography or Terreg, is narrower and possibly more practicable (as 'imminent threat' is more apparent than the fact that an 'offence that is likely to take place').

(c) Potential tension with fundamental rights

In our view, it is too early to judge whether article 18 DSA would create tension with the freedom of expression or the right to privacy of users, as it depends on how the provision will be enforced (e.g. which and how much information will be provided to the authorities, and what the authorities will do with this information). Given that the scope of article 18 DSA is potentially too broad, this may create tension with fundamental rights, namely the freedom of expression or the right to privacy of users, especially as concerns the duty to report such offences as terrorism and hate speech. With regard to hate speech in particular, as described in Section 2.2, it was suggested that the respective provisions of the German NetzDG are excessively broad and would therefore lead to infringements of the right to privacy. Thus, it would be desirable to clarify whether article 18 DSA extends to online threats and hate speech, and if so, undertake further assessment of whether and to what ex-

59 See S. Lestrade and M. Kouwenberg, 'Het vestigen van strafrechtelijke aansprakelijkheid bij online desinformatie', in this issue. For an analysis of compatibility of measures to combat hate speech online with freedom of speech on the example of German NetzDG and the draft English Online Safety Bill, see P. Coe, 'The Draft Online Safety Bill and the regulation of hate speech: have we opened Pandora's box?,' *Journal of Media Law* 2022, DOI: 10.1080/17577632.2022.2083870.

60 See Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, p. 1-14.

61 See also Gellert and Wolters 2021, p. 23-32.

62 CJEU 12 July 2011, C-324/09, ECLI:EU:C:2011:474 (*eBay*); CJEU 22 June 2021, C-682/18 and C-683/18, ECLI:EU:C:2021:503 (*YouTube*).

63 CJEU 12 July 2011, C-324/09, ECLI:EU:C:2011:474 (*eBay*); DSA compromise, Recitals 22, 42b; Gellert and Wolters 2021, p. 23.

tent hate speech should be covered, given the potential tension with fundamental rights.

(d) Effectiveness

Next to the concerns related to the scope (namely, vagueness, and as a result the possible lack of foreseeability), the effectiveness of the proposed duty of internet service providers to report crime is a matter of concern. A criticism raised in relation to the various types of duties to report crime under domestic laws, which is also potentially relevant to article 18 DSA, is that states can use laws that shift obligations to detect crime on private parties to justify lack of investment into increasing investigative capacity of law enforcement authorities.[64] It remains to be seen whether and to what extent the proposed duties under article 18 DSA will be effective to prevent, detect and prosecute serious crimes against life and safety of persons committed online.

As discussed in Section 2.1, the effectiveness of various provisions imposing duties on private actors to report crime has been questioned. The main factor impeding effectiveness of the duty to report provisions seems to be their vagueness or unclarity which leads to over- or underreporting. Given that the various elements of article 18 are open to interpretation, the risk is high that the provision might not be workable in practice. For example, it is unclear whether the information eventually supplied by hosting service providers will be sufficiently useful to lead to effective investigations and prosecutions, particularly in respect of offences such as online threats. Namely, will law enforcement authorities have the capacity to timely follow up on referrals of threats?

Furthermore, with regard to child sexual abuse, it was argued that the obligation to report to law enforcement authorities is not the most suitable measure, given the child's interests at stake (see Section 2.1).[65] Instead, reporting to an independent authority representing children, as envisaged in US and Canadian laws on online pornography described in Section 2.3, seems more appropriate.

(e) Proportionality of sanctions

Lastly, it is not clear whether sanctions attached to breaches of article 18 DSA may be considered proportionate. As stated in Section 3, sanctions for the breach of various obligations under DSA may amount to 6% of the annual profit of a service providers. These sanctions appear punitive and not restorative in nature, as the amounts in the case of very large online platforms can be very significant. As discussed in Section 2, it is questionable whether punitive sanctions are sufficiently effective in stimulating mandatory reporting. Furthermore, with regard to reporting obligations of offences that potentially encroach upon fundamental rights, such as hate speech, there is an additional risk that punitive sanctions might be considered disproportionate. At the same time, DSA appears to grant some leeway to member states to design sanctions for breaches of the specific provisions. It would be preferable to provide more clarity as to what sanctions are considered appropriate in respect of breaches of article 18 DSA in particular.

4. Conclusion

This article provides a critical analysis of the soon-to-be introduced obligation under article 18 DSA of online platforms and hosting providers to report certain criminal offences to law enforcement authorities. The analysis is based on a set of requirements which are distilled from (debates around) such laws in some domestic jurisdictions and on an EU level. A quick non-exhaustive inventory of various mandatory reporting laws demonstrates that the number of such laws is increasing. This reflects the general trend of stimulating increased involvement of private parties in law enforcement. However, the introduction of such laws runs contrary to the general legal principle that private persons should not be obliged to report crime to state authorities. Thus, such laws should be subject to stringent requirements as to their rationale(s), scope, effectiveness and proportionality (particularly, with regard to risks of encroachment on fundamental rights, and as regards sanctions for non-compliance). Assessed against these criteria, the scope and nature of obligations under article 18 DSA, as well as possible sanctions for their breach, leave room for improvement.

Although article 18 DSA seems to be grounded on clear rationales, namely the need to prevent imminent harm to life and safety of persons and to ensure more effective prosecution of crimes infringing on fundamental rights to life and personal integrity, its scope remains unclear in several respects. Further clarification is needed as to the crimes to be reported by digital service providers, which kind or level of suspicion is required to trigger the reporting obligation and what an 'offence that is likely to take place' means.

As to the question of whether article 18 DSA is effective and fit-for-purpose, we argue that the clarity of mandatory reporting provisions is directly related to their potential effectiveness, and that article 18 DSA is insufficiently clear on various points. The sanctions mentioned in article 42(3) DSA (up to 6% of annual revenue) appear disproportionate, particularly since the obligation to report (alleged) offences such as terrorism or hate speech (which potentially falls under DSA, e.g. when expressed as a threat to safety or life) can negatively affect fundamental rights, such as the freedom of expression and the right to privacy.

64 Bekker 2008.
65 Kool et al. 2021.

doi: 10.5553/BSb/266669012022003005004

We would therefore welcome more guidance from the European legislator on the various matters relevant to the scope, reporting procedure and sanctions under article 18 DSA identified in this article. Without such guidance, the mandatory crime reporting obligation of hosting service providers under the DSA is unlikely to withstand the required proportionality test under EU law.

doi: 10.5553/BSb/266669012022003005004