

INTERNET LAW AND DIGITAL SOCIETY

An International Overview



Edited by Paulina Kowalicka

INTERNET LAW AND DIGITAL SOCIETY AN INTERNATIONAL OVERVIEW

Edited By
Paulina Kowalicka

Internet Law and Digital Society: An International Overview / Edited by Paulina Kowalicka.
Milano: Milano University Press, 2025. (Information, Law & Society; 2)

ISBN 979-12-5510-207-6 (print)

ISBN 979-12-5510-210-6 (PDF)


ISBN 979-12-5510-212-0 (EPUB)

DOI 10.54103/infolawsoc.207

Quando non diversamente indicato, le pubblicazioni della collana Information, Law & Society sono soggette a un processo di revisione esterno, vengono valutate e approvate dal Comitato editoriale e devono essere conformi alla politica di revisione tra pari e alle indicazioni dell'Agenzia Nazionale di Valutazione del Sistema Universitario e della Ricerca.

Le edizioni digitali dell'opera sono rilasciate con licenza Creative Commons Attribution 4.0 - CC-BY-SA, il cui testo integrale è disponibile all'URL:
<https://creativecommons.org/licenses/by-sa/4.0>



 Le edizioni digitali online sono pubblicate in Open Access su:
<https://libri.unimi.it/index.php/milanoup>.

©The Author(s), 2025

©Milano University Press per la presente edizione

Pubblicato da:

Milano University Press

Via Festa del Perdono 7 – 20122 Milano

Sito web: <https://milanoup.unimi.it>

e-mail: redazione.milanoup@unimi.it

L'edizione cartacea del volume può essere ordinata in tutte le librerie fisiche e online ed è distribuita da Ledizioni (www.ledizioni.it)

Table of contents

Introduction	9
--------------	---

PART I

INTERNATIONAL CYBERSECURITY LAW AND COMPUTER CRIMES

Chapter I	
Challenges of Information-Sharing Under EU Cybersecurity Law: Are Competition Law and Data Protection Law: Hurdles or Enablers for Information-Sharing?	13

by Eyüp Kun

Chapter II	
Corporate Sustainability and Digitalization of Human Resources Process	25

by Claudia Ogriseg

Chapter III	
Metaverse and “Meta” Crimes, Are We Facing New Threats for People Rights?	39

by Emilio Sacchi

Chapter IV	
Harmful Contents Online and Platforms Criminal Responsibility	45

by Beatrice Panattoni

PART II

PRIVACY, DATA PROTECTION AND DATA GOVERNANCE

Chapter V	
The Lies and the Fights for Privacy: Protecting Privacy and Human Dignity in the Digital Age	55

by Elena Pagani

Chapter VI	
On the Relationship Between Competition Law and Privacy: Can we Achieve Nexus Between Competition Law and Privacy?	61
<i>by Arletta Gorecka</i>	
Chapter VII	
Assessing Risks Involved in the Use of AI Systems: Current and Future Approaches	69
<i>by Pietro Boccaccini and Taís Fernanda Blauth</i>	
Chapter VIII	
Privacy in the Digital Age: a Look at the Transformation of the Concept	85
<i>by Emanuele Brambilla</i>	
Chapter IX	
The Regulation of Data Brokers in Europe: How to Address an International Data Governance Challenge	97
<i>by Isabela Maria Rosal</i>	
Chapter X	
NFT: Privacy and Author Protection	107
<i>by Marco Alagna</i>	
Chapter XI	
Digital Inheritance in Accordance with the Right to Data Protection in the Brazilian Legal System	111
<i>by Guilherme Vargas Puchta and Zilda Mara Consalter</i>	

PART III

BIG DATA, PLATFORMS REGULATIONS AND OPEN DATA

Chapter XII	
Legal and Ethical Challenges in the Use of Web 2.0 Open Data	123
<i>by Jonida Milaj</i>	
Chapter XIII	
How Smart Cities Leverage the Power of Data and Sensors to Bridge Digital Gaps and Foster Prosperity	133
<i>by Beatrice Bonami</i>	

Chapter XIV	
Communities' Governance in WEB3: the Role of DAOs	145
<i>by María del Sagrario Navarro Lérda</i>	

Chapter XV	
Revolution of Contract Through Legal Technologies: Current Trends in Contract Automation	157
<i>by Silvia Martinelli and Carlo Rossi Chauvenet</i>	

Chapter XVI	
"Justice" on Digital Platforms: Internal Complaint-Handling Systems and Mediation in P2B Relationships. A Call for Reform	163
<i>by Ludovica Sposini</i>	

PART IV

ARTIFICIAL INTELLIGENCE, ALGORITHMS AND LEGAL TECH

Chapter XVII	
Opening Data of Smart Cities Under the DGA: an Overview of the Challenges Brought About by Data Sharing	175
<i>by Alessandra Calvi</i>	

Chapter XVIII	
The Algorithm in Administrative Decisions: Risks and Opportunities	187
<i>by Susanna Viggiani</i>	

Chapter XIX	
The AI Act Proposal: a New Right to Technical Interpretability?	195
<i>by Chiara Gallese</i>	

Chapter XX	
Innovative Versus Recurrent Perspectives on the Liability for Autonomous and Incorporated Artificial Intelligence	205
<i>by Juanita Goicovici</i>	

Chapter XXI	
Digitalisation of Justice in the EU, Challenges and Future Prospects	215
<i>by Anastasia Nefeli Vidaki</i>	

Chapter XXII

Fairness By Design: A Value-Sensitive Approach to Exploring
the Fairness Principle in the GDPR in the Context of Children's
Interaction With AI Systems

227

by Ayça Atabey

Chapter XXIII

About the Need for Regulation Central Bank Digital Currency:
Potential Monetary Legal Basis and Challenges

237

by Marko Dimitrijević

Chapter XXIV

A.I., Facial Recognition and Privacy Risk

247

by Nicolò Bottura

Chapter IV

Harmful Contents Online and Platforms Criminal Responsibility

by Beatrice Panattoni*

INDEX: 1. The context. – 2. Content-related offences. – 3. Online platforms responsibility. – 4. The contribution of criminal law to the debate on tech regulation policies.

1. The context

Life around the world is increasingly mediated by digital platforms. Individual experiences, manifestations of one's personality, and intimacy take shape through the continuous uploading and systematic sharing of data online, where bodies become screens and lives become software code. We are, in philosopher Luciano Floridi's words, "informational beings"¹.

This transition to a digital age has led to the emergence of new criminal phenomena based on both harmful contents and abuses of lawful contents, which are not always easily traceable to existing criminal offences. Content-related offences take place within and through digital communication services (social media), which have been left, until recently, without adequate legal regulation. The range of criminal offences referable to this area is significantly broad: it includes offences against public interests (such as hate speech, incitement or apology to crime and violence, dissemination of terrorist contents), and offences against a specific victim (such as forms of interpersonal hatred, non-consensual pornography, child pornography).

The scale of the dissemination of harmful contents online is quantitatively high and qualitatively severe. In many cases, they generate irreversible consequences. The technical architecture of cyberspace and content-sharing platforms (social platforms) greatly amplifies the scope and consequences of

* Postdoctoral researcher in Criminal Law at the University of Verona, Italy. She earned her Ph.D. in Criminal Law from the same University in 2022. She has been visiting scholar at the University of Freiburg (Germany), at the Max Planck Institute for the Study of Crime, Security and Law, and at the University of Washington (US). Her research investigates how digital technologies challenge theories of criminal responsibility attribution, focusing primarily on online platforms responsibility and AI-related crime.

1 Floridi, L. (2014) *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford.

communicative conducts². From a quantitative point of view, there is a fast duplication of the same or similar content, which can reach a potentially indeterminate number of recipients. From a qualitative point of view, access to and sharing of content is increasingly immediate and within everyone's reach. Given that the scale of dissemination is directly linked with both the seriousness and the frequency of the harms that might be caused by illegal contents online, tech policies could arguably require new criminal policies aimed at the prevention of such crimes³.

To develop effective measures and policies aimed at preventing content-related offences, the role of private actors which manage the social platforms where these crimes are realized is a necessary step. Therefore, an evaluation of the adequacy and efficiency of tech policies on online platform responsibility, assessing whether criminal policies, alongside other measures in place, should be included.

2. Content-related offences

A categorization of the relevant offences within the category of "content-related offence" allows giving homogeneity and systematicity to the criminal phenomenon of unlawful contents online. The choice to base the categorization on the nature and the seriousness of the harm aims to provide a standard of care to the actors liable for the removal of that content, which must be mitigated by a case-by-case analysis.

Given the breadth of the offences that might be realized through communicative conducts online, certain differentiations should be made. Specifically, we can suggest dividing content-related offences into two main clusters, based on the nature of the harm they create. The first cluster includes offences that harm public interests, such as public order or human dignity. The second cluster includes offences that harm the individual rights of a specific victim, such as her/his reputation or sexual freedom. The paper will consider, as case studies for each cluster, hate speech online on the one hand, and gender-based cyber-violence⁴ on the other hand.

2 Among studies of psychology see Aiken, M. (2017) *The Cyber Effect*, New York.

3 Digital technologies represent a facilitator in the shift of criminal law from been reactive to been based on crime control and risk avoidance. See Koops, B. (2009) 'Technology and the Crime Society: Rethinking Legal Protection', *Law, Innovation & Technology*, vol. 1(1), pp. 93-124, ILT Law & Technology Working Paper No. 010/2009.

4 Among reports addressing the topic of "cyber violence against women and girls", see: report of Sept. 24, 2015, drafted by the Broadband Commission for Digital Development, a body established in 2010 by the International Telecommunication Union (ITU) and the United Nations Educational, Scientific and Cultural Organization (UNESCO) at the behest of the then secretary-general of the United Nations; recommendation No. 35 of July 26, 2017, aimed at updating the previous Recommendation No. 19 of 1992447, prepared by the United

The circulation of violent content based on hatred toward certain minorities has exponentially increased in recent years, which was also worsened during the COVID-19 pandemic⁵. As stated by the European Agency for the Protection of Fundamental Rights (FRA), “Online hate has taken root in European societies”⁶. Given this framework, European institutions have begun to address the updating of legal sources on the subject. The definition of hate crimes and hate speech is harmonized by the Council Framework Decision 2008/913/JHA of November 28, 2008, on Combating Certain Forms and Expressions of Racism and Xenophobia by means of Criminal Law, in which manifestations of hatred based on race, colour, religion, ancestry, or national or ethnic origin are covered. However, this definition is limited, if we consider the European Convention and Charter of Human Rights (article 14 ECHR, article 21 EUCFR), where the prohibition of discrimination is extended beyond those based on racial or xenophobic grounds. The most notable gap concerns discrimination based on gender, sex, and sexual orientation.

Hate speech online is particularly affected by the technical architecture of online platforms, deepening the harm it can cause. The use of algorithmic agents that profile users can lead to opinion polarization, inducing the user to view hateful materials on a loop, as they are qualified by the algorithm as “similar” to those usually consulted by the user. Amplifying the resonance of hate content that glorifies violence creates a higher possibility that words become violent actions⁷.

Given its sudden explosion in the digital age, the need to update a European-level harmonization of the legal discipline related to hate speech, as well as its definition, has led the Commission to issue a Communication to the European Parliament and the Council with the aim of triggering a Council decision identifying hate speech and hate crimes as areas of serious and transnational crime, which meet the criteria specified in the first subparagraph of article 83(1) of the TFEU, so that substantive legislation harmonizing the definition and penalties for hate speech and hate crimes can subsequently be proposed directly

Nations Committee on the Elimination of All Forms of Discrimination against Women (CEDAW); the United Nations Special Rapporteur's Report of June 18, 2018 on Online Violence.

- 5 Numerous statistical data are reported by Peršak, N. (2022) ‘Criminalising Hate Crime and Hate Speech at EU Level: Extending the List of Eurocrimes Under Article 83(1) TFEU’, *Criminal Law Forum*, vol. 33, pp. 85-119. Available at: <https://link.springer.com/article/10.1007/s10609-022-09440-w>.
- 6 See FRA, Overview of antisemitic incidents recorded in the European Union 2009-2019, Publication Office of the European Union, 2020.
- 7 See Forti, G., Lamanuzzi, M. (2022) *Digital Violence: A Threat to Human Dignity, a Challenge to Law*, in D. E. Vigan, E., Zamagn, S., M. S. Sorond M.S. (eds.) (2022) *Changing Media in a Changing World*, Città del Vaticano, vol. 183.

by the EU⁸. Regarding this legislative initiative, the qualification of hate speech as a serious and transnational crime will have to be addressed based on the harm principle, considering it, however, from a human-centric perspective, as a crime that violates human dignity rather than the public order. A similar dramatic evolution also characterizes gender-based cyber-violence, which has many forms. They include: “online sexual and psychological harassment, cyberbullying, online stalking, non-consensual pornography, online sexist hate speech, and new forms of online harassment such as zoom bombing or online threats”⁹. As pointed out by the European Parliament, online forms of violence disproportionately affect women and girls and must be understood as an inseparable continuum from offline violence, as both are interconnected.

European institutions have begun to outline legislative policies in this area as well, which became complementary to those dedicated to countering online hate. Gender-based violence has also been identified as an area of crime that meets the criteria of article 83(1) TFEU, and the European Parliament has asked the Commission to submit a proposal for a Council decision identifying gender-based violence as a new serious and transnational crime, then using it as the legal basis for a holistic, victim-centred directive aimed at preventing and combating all forms of gender-based violence, both online and offline¹⁰.

The seriousness of specific forms of cyber-violence should not be underestimated just because these criminal conducts are perpetrated online. Violence in the digital dimension, where the victim’s “physical” body is not directly involved, may lead to a flawed criminal framing of some events, especially those involving the victim’s sexual sphere. In the field of sexual abuse through images (or non-consensual pornography)¹¹, according to the criminological theory of the so-called “embodied harm”¹², the body of the victim is equally involved in

8 Communication from the Commission to the European Parliament and the Council, A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime, 9.12.2021 COM (2021) 777 final. For a comment on the proposal see Peršak, N. (2022), ‘Criminalising Hate Crime and Hate Speech at EU Level: Extending the List of Eurocrimes Under Article 83(1) TFEU’, *Criminal Law Forum*, vol. 33, pp. 85-119. Available at: <https://link.springer.com/article/10.1007/s10609-022-09440-w>.

9 European Parliament resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime available at: [https://oeil.secure.europarl.europa.eu/oeil/cs/procedure-file?reference=2021/2035\(INI\)#gateway](https://oeil.secure.europarl.europa.eu/oeil/cs/procedure-file?reference=2021/2035(INI)#gateway).

10 Ibid.

11 See Citron, D., Franks, M. (2014) ‘Criminalizing revenge porn’, *Wake Forest Law Review*, vol. 49, p. 345, (for the US); Gillespie, A. (2015) “Trust me, it’s only for me”: ‘revenge porn’ and the criminal law’, *Criminal Law Review*, vol. 866, (for UK); and, among Italian scholars, Caletti, G. (2019) ‘Libertà e riservatezza sessuale all’epoca di internet. L’articolo 612-ter c.p. e l’incriminazione della pornografia non consensuale’, *Rivista italiana di diritto e procedura penale*, Anno LXII, Fasc. 4.

12 See Powell, A., Henry, N. (2017) *Sexual Violence in a Digital Age*, London. It elaborates, by applying sociological studies of “embodiment” (which conceive of the “body” not as mere

the criminal act. Therefore, the right harmed by these behaviours should not be reduced to confidentiality alone, whereas it should include the freedom of sexual self-determination as well.

Besides policies aimed at the direct criminalization of hate speech and gender-based cyber-violence, the complexity of the digital context requires and justifies criminal policies aimed not only at combating such crimes but also at preventing them. In addition, then, to hold responsible the users, tech policies must also look at the role and responsibilities of social platforms.

Content-related offences have been qualified also as “platform-enabled crimes”¹³, since, in many cases, their realization is enabled, facilitated, or amplified by the architecture of services offered by online platforms. Indeed, the harmfulness of unlawful contents online does not end with the uploading, it only starts from there. Recognizing legal relevance to the entire lifecycle of online information aims at understanding and analysing the criminal phenomenon in its entirety. It is precisely the persistent availability of harmful content that causes the most incisive consequences for the victim. It is from a single upload that a chain effect of sharing and further dissemination, which represent the core of the potential harmfulness of such behaviours, is most often triggered. Thus, it is what happens after the uploading that constitutes one of the most incisive innovations of the digital dimension. These stages cannot be considered legally irrelevant, they should instead be regulated.

This new scenario has led to the emergence of a protection gap in the EU and Member States’ legal systems, leaving a sector of activity as fundamental to social life as digital services without an adequate legal framework. To fill this considerable gap in legal protection, the EU institutions are following a two-way legislative strategy, aimed, on the one hand, at combating and criminalizing the dissemination of offensive materials online, and, on the other hand, at regulating the digital communication services sector by providing an apparatus of specific legal obligations to online platforms. These two policies should be understood as complementary to each other.

The operators of digital services where illicit materials circulate are the only entities able, not only to actively intervene after the information is placed online, but also to design the technical architecture that makes possible (or determines, as the case may be) the uncontrolled increase of violent, harmful, or dangerous content. Therefore, the responsibility of online platforms should not be limited to content moderation, whereas it should consider the responsibility related to the online platforms’ use of autonomous algorithmic agents in managing their

physical integrity, but as a physical, metaphysical, social and cultural phenomenon) to digital experiences, the concept of “digital-embodied harm”, according to which it is necessary to engage the corporeality of victims in the experience of cyber-violence episodes.

13 See Hamilton, R.J. (2022) ‘Platform-Enabled Crimes: Pluralizing Accountability When Social Media Companies Enable Perpetrators To Commit Atrocities’, *Boston College Law Review*.

services, and, more specifically, in indexing, filtering, and obscuring content, as provided in their internal policies.

3. Online platforms responsibility

Given that content-related offences are criminally relevant, it remains to be established whether online platforms (also defined as hosting providers)¹⁴ might be held criminally responsible for the content-related offences committed by their users.

Among Italian scholars¹⁵, it is controversial whether a platform can be held criminally liable in case of illegal contents hosted on its service. Since crimes realized by uploading illegal content online are usually considered normatively “concluded” at the moment of the “publication” of the content, no criminal liability is configurable after that moment. However, thanks to the use of new technologies and new tools (such as algorithms capable of filtering and indexing), new scenarios are opened. Starting from the category of “active” hosting provider, elaborated by the European Court of Justice¹⁶, it has become clear that the new technologies implemented by hosting providers allow a higher and stricter regime of liability, making them sort of “publishers” of the contents hosted on their platforms.

However, resorting to criminal law in this context presents several shortcomings. The technical architecture of the network and of digital communication services have an impact not only on the crimes’ harmfulness, but also on the subjective element of “intent”. If what happens after the upload of the content online (i.e., the persistent and uncontrolled circulation of the same or similar content), becomes legally relevant, it cannot in any case be considered as represented and intended by the original user who made the original upload, except resorting to forms of strict liability.

The same can be said for online platforms, whose intent is difficult to ascertain. Indeed, it would be necessary to establish that the platform’s manager had actual knowledge of the illicit content and that it intentionally failed to remove it. If we consider the large social platforms and the amount of information,

14 Hosting provider is the broader category which also include platforms. They are defined by the Digital Services Act (DSA), Regulation (EU) 2022/2065, as providers of services “consisting of the storage of information provided by, and at the request of, a recipient of the service”. See article 3 lett. g) DSA.

15 Among the most recent contributions by Italian scholars see Fiorinelli, G. (2022) ‘L’attuale ruolo del provider nella società digitale: modelli di responsabilità penale’, *La Legislazione Penale*; Lamanuzzi, M. (2021) ‘Il ‘lato oscuro della rete’. Odio e pornografia non consensuale. Ruolo e responsabilità dei gestori delle piattaforme social oltre la net neutrality’, *La Legislazione Penale*; Braschi, S. (2020) ‘Social media e responsabilità penale dell’Internet Service Provider’, *Rivista di diritto dei media*.

16 The leading case is European Court of Justice, judgment of March 23rd 2010, C-236/08 a C-238/08, Google France e Google, EU:C:2010:159.

they manage every second, it is not always possible to ascertain a malicious culpable behaviour for which they can be criminally liable. The scenario becomes even more complicated if we consider the autonomous “actions” of algorithms that “highlight” illicit content. Even for the automatic and autonomous functioning of such algorithmic “agents”¹⁷, the platform operators cannot be said to have acted with criminal intent, and therefore they cannot be considered guilty.

4. The contribution of criminal law to the debate on tech regulation policies

In the area of unlawful content online, criminal policy choices can follow two main directions, depending on the legal system taken into consideration:

1. holding criminally liable the individuals involved (e.g., the managers of the platforms);
2. holding criminally liable the corporation, also through pecuniary sanctions, seen as expressions of the broader category of “punitive law”.

The first option will present the same shortcomings that have been briefly outlined. Moreover, we need to keep in mind the specific features of the context where crimes related to digital technologies occur. Specifically, one of the main challenges of crimes related to digital technologies is that ICT’s automatic and autonomous functioning “contaminates”¹⁸ the manifestation of the *actus reus* and, consequently, they may influence also the *mens rea* requirement. This conceptual shift determines the impossibility of asking a single human agent to completely “control” what happens on digital services. Thus, in a context of “distributed moral responsibility”¹⁹, where identifying the specific sources of responsibility becomes more difficult, resorting only to individual responsibility models based on the capacity to “control” harmful outcomes is not a suitable policy option.

In the digital society, resorting only to the “traditional” concept of individual responsibility based on the capability of control over one’s own actions and their outcomes might become a dangerous policy choice. The prevention and contrast of harms related to digital technologies that fall only on citizens’

17 On the harms related to AI applications see Abbott, R., Sarch, A. (2019) ‘Punishing Artificial Intelligence: Legal Fiction or Science Fiction, in University of California’, *53 UC Davis Law Review*; Beck, S. (2016) ‘Intelligent agents and criminal law – Negligence, diffusion of liability and electronic personhood’, *Robotics and Autonomous Systems*, vol.86, pp. 138-143.

18 This suggestion is extracted from Bruno Latour’s Actor-Network Theory (ANT), which suggests that in contemporary society the action is the result of the cooperation of multiple agencies, human and non-human. Therefore, we need to shift our attention from the subject and his/her actions to the interactions that bond the different entities (persons, technology, organizations, etc.) that create a reality of network. See Latour, B. (2007) *Reassembling the Social: An Introduction to Actor-Network-Theory*, Oxford.

19 See Floridi, L., Taddeo, M. (2016) ‘The Debate on the Moral Responsibilities of Online Service Providers’, *Science and Engineering Ethics*, vol. 22(6), pp. 1575-1603.

obligations might indeed create a slippery course that does not take into account the social transformation brought about by digital technologies.

Given the described shortcomings, criminal law might aim at its self-containment in this area of regulation, leaving it only to alternative measures, such as administrative sanctions. However, excluding criminal law completely from the set of policies could miss the opportunity to take advantage of the affirmative contribution it could bring in shaping responsibility models through its principles and guarantees, first and foremost the principle of culpability, without which these policies could become mere formal orders to be complied with, lacking an impact in terms of prevention and re-education.

Therefore, the second policy option seems more suitable. Grounding responsibility not on single persons but on corporations could provide more effective legal protection, as well as increase trust in digital technologies by creating a framework based on the proactive cooperation between the different stakeholders involved (the public, private actors, and authorities). Therefore, accountability models based on punitive law²⁰, which mitigate the “paradigm of control”, might bring a significant contribution to the definition of the set of tech policies on platform-enabled crimes.

Despite which path will be chosen by national legislators, tech policies should avoid holding platforms indirectly responsible for the crime of their users, whereas they should hold them directly accountable for the guilty management of their service. This is also the approach followed by the EU Regulation on digital services (DSA)²¹, which regulates several due diligence obligations, not aimed at preventing an unlawful event, but at setting a standard of care that is both adequate and socially accepted for large platforms, based on a virtuous organization of their services and businesses²².

20 Wrongdoings punished with administrative sanctions that, due to the “suffering” they impose, preserve a punitive nature. On the topic see Dyson, M., B. Vogel, B. (eds.) (2018) *The limits of criminal law*, Cambridge.

21 See footnote n. 14.

22 See Montagnani, M.L. (2020) *A new liability regime for illegal content in the digital single market strategy*, in G. Frosio (eds.), *Oxford Handbook of Online Intermediary Liability*, Oxford, p. 399. The DSA provides for different sets of positive obligations for hosting providers, which increase in number and complexity according to the type of provider. The most stringent set of obligations concerns large platforms (with an average monthly number of active users of 45 million or more). These private actors will be obligated to set up a system for assessing and managing the “systemic risks” associated with their services, including the risk of dissemination of illegal content through their services (article 33 DSA).