Online Platforms in the Cybersecurity System

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ

Abstract The issue of cyberspace security is determined by the development of new technologies, including robotics and digital processes, and the state's computerisation progress. The fundamental issue of legal protection in the cybersecurity system is to determine the subjective and objective scope of responsibility for online activities. One of the key regulations regarding liability in the field of cybersecurity is the NIS Directive and its draft amendment, the so-called NIS 2. Technological change in the field of communication has fundamentally modified the ways individuals and entire communities function. It should be ensured that hosting service providers process the received counter-notices in the proper manner. As a result of technological and economic convergence, the same entity may perform very different functions, and it is not determined what its status will be, so the scope of its liability is not conclusively determined. The situation calls for appropriate regulations, with the reservation that there is a need to synchronise issues at each stage of legislative activity.

Keywords: • cybersecurity • cyberspace • online platforms • digital services • e-services • digital content • responsibility • liability • digital infrastructure

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Associate Professor, War Studies University in Warsaw, Law Institute, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland; Head of the Academic Centre for Cybersecurity Policy, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: kasiachalubinska@gmail.com.

https://doi.org/10.4335/2022.2.1 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Duties and responsibilities

The notion of network security or cybersecurity covers, *inter alia*, the protection of resources – data, information and, more generally, digital content, the protection of ICT networks and devices, i.e., computers, and also the protection of content transmission via networks, so the communication process itself. The human factor is also worth noting here, namely the protection of network and computer users. It should definitely be stressed that human activity is still an important element in the process, and this is perhaps one of the underlying dilemmas regarding the future of cybersecurity.

The issue of cyberspace security is determined by the development of new technologies, including robotics and digital processes, and the state's computerisation progress. The latter is a key element for the development of cybersecurity administration which can be perceived from two different angles. The first may refer to cybersecurity administration in the objective sense, concerning a specific group of institutions with certain competences and tasks, while the second is connected with positive law applied with a view to implementing the state's cybersecurity mission, goals and tasks, both nationally or internationally. It is worth stressing that legal provisions which can be nowadays classified as those regulating the issue of cybersecurity are very often dispersed and cover different areas of human life. The issue of such dispersion was not successfully resolved by the National Cybersecurity System Act of 5 July 2018 (Journal of Laws of 2018, item 1560) (hereinafter: the National System Act) implementing the NIS Directive into Polish legislation. Nonetheless, it should be emphasised that the fundamental issue of legal protection in the cybersecurity system is to determine the subjective and objective scope of responsibility for online activities. First and foremost, however, it is necessary to define what digital content is and when it can be deemed illegal, as well as to answer the question of who bears liability for it and to what extent.

2 Duties of digital providers in light of the NIS Directive and the National Cybersecurity System Act

One of the key regulations regarding liability in the field of cybersecurity is the NIS Directive and its draft amendment, the so-called NIS 2, which is meant to replace the original act, so as "to address the increased interconnectedness between the physical and digital world through a legislative framework with robust resilience measures, both for cyber and physical aspects as set out in the EU Security Union Strategy" (COM(2020) 605). The amendment is aimed at increasing the resilience of "essential actors" and "relevant actors" reaching certain thresholds in numerous sectors against all threats connected with information and communication technologies (ICTs). The opportunities offered by new technologies and the need to properly adjust the administrative and legal system are crucial issues for the development of modern ICT network security management. Public authorities are now obliged to provide electronic services to citizens, covering both citizen services and other areas of public administration, not excluding the decision-making process. The impact of new technical means which were introduced into

public administration forces some changes in basic administrative and legal relations (individual-citizen), and is of great significance for the inter-sector cooperation in the course of the implementation of public tasks. Cyberspace is a new domain of impact exerted by these processes. Along with the development of cyberspace, the threats which are connected with it also evolve. Currently, cyberspace is a symbol of development, but also of freedom and privacy, and any interference in its functioning tends to be viewed as an attack on these values. However, in the states engaged in building an information society, cybersecurity is considered one of the most serious challenges for the national security system. It refers to the security of both the entire state institution and individual citizens. The responsibility for ensuring cybersecurity applies to all network users, but a significant role is played by public administration bodies whose basic tasks include taking measures to ensure security and public order. As part of arranging for the implementation of public tasks oriented towards ensuring national security, with particular emphasis on the definition of public tasks in the field of critical infrastructure protection, it is important to establish a list of entities carrying out public tasks in the field of cybersecurity. It should be remarked that these entities may include public entities performing public tasks, private entities performing public tasks due to the privatisation of public task performance, and private entities performing their own tasks which are of particular importance for the public interest, or which were once performed as public tasks but were then subject to privatisation. In consequence, the issue of inter-sector cooperation becomes significant in the process of establishing a unified cybersecurity system. This platform has given rise to certain measures and more intensive cooperation between the public and private sectors as regards the identification of key resources, means, functions and underlying requirements for resilience, as well as the need for cooperation and mechanisms to respond to large-scale disruptions of electronic communications. For this reason, digital service providers are becoming a major element of the EU cybersecurity system.

Digital service providers are legal persons or organisational units without legal personality having their registered office or management board in the territory of the Republic of Poland, or acting via a representative having its organisational unit in the territory of the Republic of Poland, providing digital services, including services rendered by electronic means, within the meaning of the Act on the Provision of Services by Electronic Means. Legal commentators separately distinguish entities providing digital services. J. Barta and R. Markiewicz distinguish the following categories of entities: telecommunication network holders/operators – telecommunication companies; access providers – entities providing services which consist in enabling access to the network without any influence on the content transmitted through that network; primary network content providers, content providers – entities whose activity consists in introducing their "own" content into the network, which allows other users to use this material; and network service providers (service providers) (Barta, 2014:213-215). (More information in Gęsicka 2014:40-49). M. Zieliński distinguishes three categories of entities falling within the service provider category, i.e., access providers, network providers and intermediary service providers. He also mentions content providers (Zieliński: 2013:38).

A similar distinction is applied by Litwiński (2004:176-178). The legislator excluded from the application of the Act those entrepreneurs (micro- and small entrepreneurs) who are referred to in Article 7(1)(1) and (2) of the Act of 6 March 2018 – Entrepreneurs Law (Journal of Laws of 2021, item 162, 2105).

The notion of e-service, which is given a similar meaning to that attributable to the notion of information society services in Directive 2000/31/EC, is related to the concept of digital services, including those provided by electronic means. This service was defined as a service provided in an automated manner through the use of information technology, by means of ICT systems on public telecommunications networks, at the individual request of the service recipient, without the simultaneous presence of the parties in the same location; however, e-services do not include: a) radio and television broadcasting services, b) telecommunications services, c) the supply of the following goods and services: goods in the case of which the ordering and order processing is done electronically, CD-ROMs, floppy disks and similar physical media, printed material such as books, bulletins, newspapers and magazines, CDs, cassettes, video tapes, DVDs, games on CD-ROM, services provided by lawyers or financial advisers who offer advice by e-mail, educational services during which the course content is delivered by the instructor via the internet or an electronic network (i.e., remotely), off-line physical repair services of computer equipment, off-line data warehousing, advertising services, in particular in newspapers, on posters and on television, call centres, educational services provided by correspondence, especially through the post, conventional auction house services involving human intervention, irrespective of the bid submission mode, telephone services with a video component, access to the internet and websites, and telephone services provided via the internet. In the Regulation of the Minister of Regional Development of 21 March 2013 on granting financial aid by the Polish Agency for Enterprise Development to support the establishing and development of electronic economy under the Operational Programme Innovative Economy 2007-2013, e-service was defined as a service provided in an automated manner, with the use of information technology, by means of ICT systems in public telecommunications networks, at the individual request of a recipient of services, without the simultaneous presence of the parties in the same location; however, e-services do not include: a) radio and television broadcasting services, b) telecommunication services, c) the supply of the following goods and services: – goods in the case of which the ordering and order processing is done electronically, – mobile computer storage media, – printed material such as books, bulletins, newspapers and magazines, – sound recordings on analogue or computer storage media, – audio and video recordings on analogue or computer storage media, – computer games on computer storage media, – services provided by means of electronic communication, – educational services during which the course content is delivered by the instructor by means of electronic communication, – advertising services, in particular in newspapers, on posters and on television, – call centres, – educational services provided by correspondence, especially through the post, – conventional auction house services involving human intervention, irrespective of the bid submission mode, –

telephone services with a video component, – access to the internet, – telephone services provided via the internet (Journal of Laws of 2013, item 412).

In accordance with Article 2 (2) of Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services, a digital service means (a) a service that allows the consumer to create, process, store or access data in digital form, or (b) a service that allows the sharing of, or any other interaction with, data in digital form uploaded or created by the consumer or other users of that service, or other forms of interaction using such data. This definition incorporates both an element of the creative process of digital content and of its use. The extension of the definition of information society service providers will include internet service providers, cloud computing, domain name system service providers, social media, search engines, collaborative economy platforms, online advertising services, blockchain-based services. These are commonly referred to as ISPs (internet service providers), and these types of providers are already covered by sector-specific provisions, including the new European Electronic Communications Code (Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, p. 36) and Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the BEREC Support Agency (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No. 1211/2009 (OJ L 321, p. 1), which is currently being implemented in EU countries. The global reach of digital services materially contributes to the fact that there is no full standardisation of legal relations relating to their provision. These are cross-border services, and domestic law cannot influence the services rendered by service providers from other countries. This also applies to the National Cybersecurity System Act although the Polish legislator has stipulated that the rules relating to cybersecurity obligations shall apply to a legal person or an organisational unit without legal personality having its registered office or management board in the Republic of Poland, or acting via a representative having its organisational unit in the Republic of Poland, provided that the digital service provider which does not have an organisational unit in one of the Member States of the European Union, but offers digital services in the Republic of Poland, shall appoint a representative having its organisational unit in the territory of the Republic of Poland, unless it has already appointed a representative having its organisational unit in another Member State of the European Union. A representative may be a natural person, a legal person or an organisational unit without legal personality, established in the Republic of Poland or in another European Union Member State, appointed to act on behalf of the digital service provider that does not have an organisational unit in the European Union, whom the authority competent for cybersecurity, the CSIRT MON, the CSIRT NASK or the CSIRT GOV may refer to in connection with the digital service provider's obligations under the Act. The definition of a digital service and the specification of its objectives will have an impact on determining the responsibility for the tasks which entail responsibility. This is how it was also envisaged in the draft Digital Services Act (Proposal – 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.), under which digital services comprise a large category of online services, ranging from simple websites to online infrastructure services and online platforms. The principles set out in the draft of the Digital Services Act primarily concern online intermediaries and online platforms, such as online marketplaces, social networking sites, content sharing platforms, app stores, and online travel and accommodation platforms. In turn, the draft Digital Markets Act (Proposal – Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final) contains provisions governing online "gatekeeper" platforms. Gatekeeper platforms are digital platforms playing a systemic role in the internal market, which function as bottlenecks between businesses and consumers in the case of important digital services. Some of these services are also regulated under the Digital Services Act, but for different reasons and to different extents.

The types of digital services to which the reference regulation applies are set out in Annex 2 to the National Cybersecurity System Act. These are: **an online marketplace** – a service enabling consumers or traders to enter into contracts electronically with traders in an online marketplace or on the website of the trader who uses services provided by the online marketplace (e.g., Allegro, ING Usługi dla Biznesu S.A. – ALEO.COM, B2B automicob2b.pl platforms); **a cloud computing service** – a service enabling access to a scalable and flexible set of computing resources for a shared use by multiple users (such as Cloud for Business – ergonet.pl, Amazon Web Services, Google Cloud Platform, Microsoft Azure, private and hybrid clouds) and **a search engine** – a service enabling users to search all web pages or websites in a given language by entering a keyword, a phrase or another element as a query, and then presenting links that refer to information connected with the query. The users of digital services should encompass natural and legal persons who are customers of, or subscribers to, an online marketplace or a cloud computing service, or who are visitors to an online search engine website in order to undertake keyword searches (Commission Implementing Regulation (EU) 2018/151). The measures to be launched by digital service providers must ensure a level of cybersecurity appropriate to the risk, taking into account the following elements: 1) the security of systems and facilities; 2) incident handling; 3) business continuity management; 4) monitoring, auditing and testing; 5) state of the art, including compliance with international standards, as referred to in Commission Implementing Regulation (EU) 2018/151.

When analysing cybersecurity issues in the context of responsibility for the security of digital services, it is important to pay attention to the transmission of data and information by electronic means, the ICT network. One can say that cybersecurity law, including that dealing with the security of the information itself, touches upon issues related to the legal protection of the ICT system that contains certain data enabling the provision of digital services, the protection of the electronic services themselves and related content and databases, as well as the network through which the transmission of such services takes place. Therefore, it should be assumed that cybersecurity is closely related to the notions

of information and telecommunication security, and more specifically to ICT security, which means the protection of information processed, stored and transmitted using ICT systems against undesired (either accidental or intentional) disclosure, modification or destruction, or against rendering its processing impossible. Digital service providers may submit to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV information regarding: 1) other incidents; 2) cyber threats; 3) risk estimation; 4) vulnerabilities; and 5) technologies used. "Cyber threat" means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons (Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1 OJ L 151, 7.6.2019, pp. 15–69). This is not a mandatory obligation, but it is related to the possibility of ensuring the fulfilment of other tasks of the digital service provider, which, through the scope of the information provided, can contribute to improving the level of cybersecurity.

3 Digital infrastructure and the proposal for a CER Directive

Another area of future regulations covering the duties and responsibilities of online platforms is the area of crisis management. The Proposal for a Directive of the European Parliament and of the Council on the critical entities resilience (CER) of 16 December 2020 COM(2020) 829 final 2020/0365(COD). As is stressed by the EU legislator in the Proposal, "the current framework on critical infrastructure protection is not sufficient to address the current challenges to critical infrastructures and the entities that operate them. Given the increasing interconnection among infrastructures, networks and operators delivering essential services across the internal market, it is necessary to fundamentally switch the current approach from protecting specific assets towards reinforcing the resilience of the critical entities that operate them". The Proposal, therefore, introduces new duties to adopt certain measures to ensure the provision of services which are essential for the maintenance of vital societal functions or economic activities within the internal market, and in particular to identify critical entities and to enable them to comply with specific obligations in order to increase their resilience and improve their ability to provide these services within the internal market. The Directive also establishes rules on the supervision and the enforcement of critical entities and the specific oversight of critical entities considered to be of particular European significance. Article 1 further explains the relationship between the directive and other relevant acts of Union law, and the conditions under which information that is confidential pursuant to Union and national rules shall be exchanged with the Commission and other relevant authorities. These duties relate to the so-called digital infrastructure which includes, according to the subjective definition, providers of cloud computing service (referred to in point (X) of Article 4 of NIS 2 Directive); providers of data centre service (referred to in point (X) of Article 4 of NIS 2 Directive); and providers of content delivery network (referred to in point (X) of

Article 4 of NIS 2 Directive). A content delivery network is a network of servers that deliver websites and other content to users.

4 Responsibility of online platforms for digital content

The processes of the convergence of digital media with traditional media has given rise to a particular type of conflict regarding arrangements for the scope and level of new regulations, particularly with respect to digital content in the case of which most issues relate to new media and new technologies (the protection of intellectual property, protection of national identity, right to privacy, the protection of children and young people), as well as in the economic field (control of the media market and the responsibility of digital service providers). New content management models are seen to emerge (including online), supported by new principles of virtual organisation.

Technological change in the field of communication has fundamentally modified the ways individuals and entire communities function. Online multimedia platforms providing electronic services are being launched, which require the use of modern technological solutions, with investments being most frequently made by entities operating in the private sector. An open and free cyberspace allows the exchange of cultures and experiences between countries, communities and citizens, enabling interaction and the sharing of content and, in consequence, also knowledge, experiences and technologies. The ideological basis supporting this exchange is the freedom of speech and the freedom of communication. Digital reality facilitates the implementation of public tasks in a new social dimension (On the redefinition of public interest in the new media, see Chałubińska-Jentkiewicz, Nowikowska, Wąsowski, 2020). The new technological order constitutes the premise and, at the same time, the subject of the discussed changes, which fundamentally impact on the regulatory area of digital media. The issue of regulating this domain of activity refers to several main levels. The activity of digital content providers entails making that content available through ICT systems. This category is strongly diversified, covering not only specialised institutions or entities but also end users. The latter group is particularly active due to the growing popularity of user-generated sites (or user-generated content). Due to their intensive activities online, content providers bear direct liability for any infringements resulting from such activities.

In the current Polish legal system, content providers also bear direct liability for infringements upon third-party rights. As noted by J. Barta and R. Markiewicz, attempts to classify the activities consisting in making works available in computer networks gave rise to controversies, and these activities were eventually qualified as a new field of use, i.e., making a work available in such a way that everybody could access it at a time and place chosen by them. In ICT networks, the functioning of which is based on interactivity, this issue was of significant importance, while the modification of content and its further dissemination by users, in the course of digital processes, did not prove troublesome. The concept of *sui generis* protection of the rights of the producer or provider of content on the network appears interesting.

5 The liability of digital content intermediaries

As regards other infringements, content providers were considered parties directly committing the infringement and were thus excluded from the limitation of liability of providers of electronically supplied services. Not only did technological changes influence the scope of liability for illegal acts in cyberspace, but also new rules emerged to limit that liability. In European law, the liability of internet service providers is regulated by way of Directive 2000/31/EC, which contains provisions regarding the most popular network services: *mere conduit*, *caching* and *hosting*. Similar rules of liability were also upheld in the proposed Digital Services Act. It should be noted that the European regulation follows the horizontal model, meaning that the exemptions it provides for apply to any legal liability, including civil, criminal, and administrative liability. Directive 2000/31/EC on Electronic Commerce lays down the rules for excluding liability at the maximum level. Consequently, individual Member States may decide to impose less strict solutions. The provisions of Directive 2000/31/EC on Electronic Commerce were transferred into Polish law by way of Articles 12–15 of the APSEM. Under Article 12 of that Act, relating to mere conduit, "the service provider that provides services by electronic means involving transmission in a telecommunications network of data shared by the recipient of the service or the provision of access to a telecommunications network, within the meaning of the Act of the 16 July 2004 – Telecommunications Law, shall not bear responsibility for the conveyed data if: 1) it is not an initiator of the transmission; 2) does not select the recipient of data; and 3) does not delete or modify the data being subject to transmission". The releasing from responsibility, referred to in paragraph one, also covers automated and short-term indirect storage of the transmitted data, if this activity aims exclusively at proceeding with transmission, and the data are not stored longer than necessary for the accomplishment of the transmission in ordinary conditions (Article 12(2) of the APSEM).

6 Editorial responsibility for digital content

The basic regulatory provisions on the digital media market, and in particular large corporations (online platforms), were laid down in the First Amendment to the U.S. Constitution, where it was established that Congress should make no law restricting the freedom of speech or the freedom of the press, and in Article 230 of the Communications Decency Act (47 U.S. Code), which reads that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". This provision ultimately stipulated that the intermediary does not bear editorial responsibility for the content it shares when providing a digital service. Therefore, this rule is equally applicable to all activities related to a platforms operation in the context of the American law by which they are governed. However, it should be noted that, also in the context of libel, certain legal acts have been issued, such as Rachel's Law (in New York State, in connection with the case of Dr Rachel Ehrenfeld, an American researcher who was sued in London by a Saudi

businessman and his two sons over a book which, although not published in the UK, was sold in 23 copies via the internet and one chapter was made available online (cf. Garton Ash, 2018: 48–49). In Ehrenfeld v. Mahout, the Supreme Court of the New York State held that the law would not protect Dr Ehrenfeld from a British lawsuit filed by Saudi billionaire Khalid Salim Bin Mahfouz, where she was ordered to pay over $225,000 in damages and legal fees to Bin Mahfouz, as well as to apologise and destroy existing copies of her books), and the SPEECH Act (Libel Terrorism Protection Act, S.6687/A.9652), which protects American citizens from the impact of foreign libel judgements if these fail to satisfy the First Amendment or procedural standards. According to R. Lancman: "This law will give New York's journalists, authors, and press the protection and tools they need to continue to fearlessly expose the truth about terrorism and its enablers, and to maintain New York's place as the free speech capital of the world" (cf. Garton Ash 2018:48-49).

It should further be noted that on29 April 2021 the European Parliament and the Council of the EU adopted a regulation to prevent the online dissemination of terrorist content (Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (OJ EU L 172, p. 79). The Regulation is to take effect in 2022. It stipulates that domestic bodies responsible for countering terrorism will not need to obtain prior judicial authorisation to order the removal of terrorist content, and a domestic body of a Member State will be able to demand the removal of content uploaded on a platform belonging to any provider rendering its services within the EU in all EU countries. An obligation was introduced for platforms to remove terrorist content within one hour (unless this is deemed impossible due to "technical issues").

An exception was made for educational, journalistic, scientific, artistic and other content whose purpose is not to promote terrorism but to spread awareness of the dangers of terrorism. The underlying issue is whether automated filters will be capable of distinguishing such content from genuinely harmful publications. The Regulation introduces a mechanism of appealing against unjust decisions to remove content (which is, in principle, intended to enable restoring such content and thus counteracting the phenomenon of excessive and arbitrary blocking) and an obligation for internet corporations to publish reports (allowing for the monitoring of how the Regulation will be applied in practice). As previously mentioned, the Digital Services Act introduces new general rules on the liability of, *inter alia*, platforms for content added by their users, this change being consistent when it comes to the liability of intermediaries on the digital services market. In accordance with the new regulations, platforms will have a maximum of one hour to remove or block access to content marked as terrorist content (including texts, photos, audio or video recordings that incite, abet or contribute to terrorist crime, contain instructions facilitating the commission of terrorist crime or incite participation in a terrorist group). This implies that although platforms will not be under the obligation to monitor or filter content on an ongoing basis, if the domestic bodies identify a site as being particularly exposed to terrorist propaganda, it will be obligatory to take measures

to prevent the publication of such content. The Regulation, however, does not specify in detail the measures to be taken, so it will be up to the platform whether it decides to use algorithms to filter content or hire moderators to do so.

The responsibility of a content-sharing internet-portal administrator for users' comments appears equally doubtful. More specifically, doubts arise as to the qualification of such comments as press material within the meaning of Article 7 (2)(1), and (4) & (5) of the Press Law. Press material means any text or image published or submitted to a publication, whether informative, journalistic, documentary, or other, regardless of the media means, type, form, destination, or authorship. At the same time, based on the applicable legislation, the press is construed as including periodical publications which do not constitute a limitative or homogeneous entirety, are published at least once a year, and bear a permanent title or a name, a number and a date, including in particular daily newspapers and magazines, news wires, telex messages, bulletins, radio and television broadcasts, or newsreels. It also covers any means of mass media, existing and emerging in the course of technological advancement, including broadcasting stations and PA systems, which distribute periodical publications via print, video, audio, or any other broadcasting means, as well as teams of people and individuals engaging in journalistic activity.

In this context, Strasbourg case law uses the term "public watchdog" when referring to the vital role played by the press. The principle that the freedom of expression, and the resulting free public debate, constitutes one of the essential foundations of a democratic society, and one of the basic conditions for its progress, and for every individual's self-fulfilment, forms one of the case-law principles adopted by the European Court of Human Rights. However, in case 5493/72, Handyside v. the United Kingdom (ECHR Judgement of 17 December 1976, 5493/72, Handyside v. the United Kingdom, HUDOC), the Court ruled that the freedom of expression was applicable not only to information or ideas which are favourably received or regarded as inoffensive, or as a matter of indifference, but also to those which offend, shock, or disturb the State, or any sector of the population. Such are the demands of the pluralism, tolerance, and broadmindedness, without which there is no democratic society. A similar view was highlighted by the Court of Justice of the European Union under Article 10 of the European Convention on Human Rights, and in Article 11(1) of the Charter of Fundamental Rights (cf. Judgements of the Court of Justice of 6 March 2021, C-274/99 P, Bernard Connolly v. the European Commission EU:C:2001:127; Judgement of 13 December 2001, C-340/00 P, the European Commission v. Michael Cwik, EU:C:2001:701; of 6 September 2011, C-163/10, criminal proceedings against Aldo Patriciello, EU:C:2011:543; Judgement of 3September 2014, C-201/13, Johan Deckmyn and Vrijheidsfonds VZW v. Helena Vandersteen et al., EU:C:2014:2132.). The same view should also be considered to form part of the case law of the Constitutional Tribunal of the Republic of Poland (cf. Judgements of the Constitutional Tribunal of 23 March 2006, K 4/06, OTK-A 2006/3, item 32; of 11 October 2006, P 3/06, OTK-A 2006/9, item 121; of 30 October 2006, P 10/06, OTK-A 2006/9,

item 128; of 14 December 2011, SK 42/09, OTK-A 2011/10, item 118; of 25 February 2014, SK 65/12, OTK-A 2014/2, item 14).

This view is shared in the rulings of the Supreme Court. It is indicated that a journalist's obligation to exercise diligence and accuracy arising from Article 12(1) of the Press Law Act (the Press Law Act refers to due diligence and accuracy) means qualified diligence and accuracy which takes into consideration the actual role of the media in a democratic society, and in their tangible impact on public opinion, and hence the emerging threats to the information autonomy and moral rights of individual people (see Resolution of the Supreme Court (7) of 18 February 2005, III CZP 53/04, LEX No. 143120). Also in the rulings of the Constitutional Tribunal, the emphasis is on the significant correlation and interrelation of the media's freedom of expression, and their responsibility for exercising that freedom, as well as the resulting need to ensure the appropriate protection of other constitutional values, including the moral rights of third parties (see in particular the judgements of the Constitutional Tribunal of 12 May 2005, SK 43/05, OTK-A 2008/4, item 57, and of 30 October 2006, P 10/06, OTK-A 2006/9, item 128).

Considering the above, in the judgement passed in case 64569/09, Delfi v. Estonia (ECHR Judgement of 16 June 2015, 64569/09, Delfi AS v. Estonia, LEX No. 1730680), the European Court of Human Rights ruled that making the internet news portal responsible for offensive comments posted on its site was legitimate. The court thus claimed that, notwithstanding the provisions of Directive 2000/31/EC on Electronic Commerce, specific solutions might be adopted in domestic law limiting the freedom of expression if the internet users' comments are offensive or hateful, and the portal administrator has failed to prevent their publishing, has derived benefits from such publishing, and has ensured the anonymity of their authors. Under that interpretation, the exclusions made in Articles 12–15 of the APSEM are subject to analysis, including in the context of other regulations governing the protection of human rights and freedoms.

Due to the fact that comments posted by anonymous authors on an online portal administrated by a website can include content violating moral rights, the responsibility in the context of violating the provisions of Article 24 § 1 of the Civil Code should be subject to scrutiny. The Supreme Court, in its judgement of 30September 2016, I CSK 598/15 (LEX No. 2151458), adopted the view that the provisions of Article 14(1) and (15) of the APSEM govern issues related to the exclusion of the online portal administrator's liability, but they fail to regulate such issues as apportioning the burden of proof, and the absence of illegality of actions of the online portal administrator rendering hosting services. The Supreme Court highlighted that, under Article 24 § 1 of the Civil Code, any person whose personal interests are threatened by another person's actions may demand that these actions be ceased. If there is an infringement, he or she may also demand that the person committing the infringement take the necessary steps to remove its effects, in particular that the person makes a statement of the appropriate form and substance. Moreover, Article 24 § 1 of the Civil Code does not restrict its applicability to parties directly committing the infringement of moral rights, who in this case are

anonymous authors, but also covers all the activities of entities which in any way infringe or contribute to infringing the moral rights of the aggrieved party, or aggravate the infringement of such rights caused previously by other entities (under this provision, the notion of the party committing the infringement of moral rights is broad enough to make referring to Article 422 of the Civil Code unnecessary). The Supreme Court noted that the freedom of expression exercised on internet fora by anonymous authors often provokes uncontrollable expressions which evolve into hate speech infringing on the moral rights of third parties. Finally, the Supreme Court stressed that individuals who are offended and slandered in anonymous posts, when the liability of the parties who directly commit the infringement is excluded, find themselves at a particularly greater legal disadvantage. "Such an aggrieved party does not even have to have access to the internet, or "read" websites, or spend their time looking for posts which are offensive or slanderous to them, or which undermine their authority. It is possible that an individual who does not use the internet might even never learn about the illegal anonymous posts about him or her which irreversibly undermine their integrity. The internet is a medium which should be friendly to the information society by design. Therefore, effective legal mechanisms should be in place to prevent the use of the internet for insulting the dignity and honour of citizens without any legal consequences for the perpetrators". Accordingly, the defending party bears the burden of proof that before the lawsuit was served, it had had no knowledge of the incriminating comments posted by internet users.

It needs to be stressed that the exclusion of civil-law liability is governed both by Article 24 § 1 of the Civil Code, and the aforementioned Article 14(1) and Article 15 of the APSEM. Assessing the interrelation of these provisions, therefore, appeared justified. However, the Supreme Court decided not to make that assessment, which influenced its judgement. This extended interpretation might seem contradictory to the conflict-of-law rules, the principle of legal-system consistency, and the interpretation of the objectives of the provisions, both as regards Directive 2000/31/EC on Electronic Commerce and the Act on the Provision of Services by Electronic Means. In this context, the provision of Article 14(1) of the APSEM might appear groundless. However, the justification of the above-mentioned ruling is congruent with the recent Commission Recommendation (EU) which deals with the monitoring of content made available as part of a hosting service. Pursuant to Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online, provisions should be made for mechanisms to submit notices. These mechanisms should be easy to access, user-friendly and should allow the submission of notices by electronic means. More specifically, these mechanisms should allow the submission of notices which are sufficiently precise and adequately substantiated to enable the hosting provider concerned to take an informed and diligent decision in respect of the content to which a given notice relates, in particular whether or not that content is to be considered illegal, and whether or not it is to be removed or access thereto is to be disabled. These mechanisms should be such as to facilitate the provision of notices that contain an explanation of the reasons why the notice provider considers that content to be illegal and a clear indication of the location of that content. Where the notice providers decide to do so, their anonymity should be ensured towards the content

provider. Where a hosting service provider decides to remove or disable access to any content that it stores because it considers the content to be illegal, irrespective of the means used for detecting, identifying or removing or disabling of access to that content, and where the contact details of the content provider are known to the hosting service provider, the content provider should, without undue delay, be informed in a proportionate manner of that decision and of reasons for taking it, as well as of the possibility to contest such a decision. Content providers should be given the possibility to dispute the decision by the hosting service provider, at a reasonable time, through the submission of a counter-notice to that hosting service provider. The mechanism to submit such counter-notices should be user-friendly, and allow their submission by electronic means.

It should be ensured that hosting service providers process the received counter-notices in the proper manner. When the counter-notice contains grounds for the hosting service provider to consider that the content to which the counter-notice relates is not to be considered illegal, it should reverse its decision to remove or disable access to that content without undue delay, without prejudice to its possibility to set and enforce its terms of service in accordance with Union law and the laws of the Member States. Hosting service providers should be encouraged to take, wherever appropriate, proportional and specific proactive measures in relation to illegal content. Such proactive measures could involve the use of automated means for the detection of illegal content only where appropriate and proportionate, subject to effective and appropriate safeguards. The removal of content which is not illegal should be precluded, without prejudice to the possibility for hosting service providers to set and enforce their terms of service in accordance with Union law and the laws of the Member States. To this end, there should be effective and appropriate safeguards ensuring that hosting service providers act in a diligent and proportionate manner in respect of content that they store, in particular when processing notices and counter-notices and when deciding on the possible removal of or the disabling of access to content considered to be illegal content.

Where hosting service providers use automated means in respect of the content they store, effective and appropriate safeguards should be provided to ensure that decisions taken concerning that content, in particular decisions to remove or disable access to content considered to be illegal, are accurate and well-founded. The document also contains detailed recommendations concerning terrorist content. Hosting service providers should expressly set out in their terms of service that they will not store illegal content and should take measures so that they do not store terrorist content.

7 The proposed Digital Services Act – new rules of liability of digital content intermediaries

The proposed Digital Services Act retained the rules of liability of network service providers and intermediaries, laid down in Directive 2000/31/EC on Electronic Commerce which is considered the basis for the digital economy. Nevertheless, to ensure

an effective harmonisation across the European Union and to avoid legal fragmentation, it was considered necessary to include these rules in the regulation. It was also deemed appropriate to clarify some aspects of these rules to eliminate the existing disincentives towards voluntary own-investigations undertaken by providers of intermediary services in order to ensure their users' safety, and to clarify their role from the perspective of consumers in certain circumstances. Chapter II of the proposed Act contains provisions on the exemption from liability of providers of intermediary services. More specifically, it stipulates the conditions under which providers of mere conduit (Article 3), caching (Article 4), and hosting services (Article 5) are exempt from liability for the third-party information they transmit and store.

The proposed DSA introduces the following regulations:

- measures against illegal goods, services, or content on the internet, such as a mechanism enabling users to flag such content, and, as regards platforms, a mechanism for cooperation with "trusted flaggers",
- new duties related to the traceability of business users of online marketplaces in order to make it easier to trace the sellers of illegal goods,
- effective safeguards for users, including the possibility to contest a platform's decisions regarding content moderation,
- extensive measures to ensure the transparency of online platform operations, including algorithms used for prompts,
- duties imposed on very large platforms to prevent the improper use of their systems by taking measures based on risk assessment, and by conducting independent inspections in connection with systems risk management,
- ensuring that the largest platforms provide scientists with the most important data in order to facilitate research into how threats evolve on the net,
- a supervisory structure matching the complexity of online space: EU countries will play a major role, supported by the new European Council for Digital Services, and in the case of very large platforms – enhanced supervision and provisions enforcement by the Commission.

It was noted in the Regulation that the platforms are deemed obligated if their reach exceeds 10% of the European population, i.e., 450 million consumers.

The proposed Act also introduces the previously known rules of limited liability for content in cases of mere conduit, caching, and hosting.

The proposed Act also introduces a rule stating that exemptions from liability of the providers of intermediary services should not be waived if they carry out voluntary or legally required own-initiative investigations (Article 6). The proposed Act further provides that no general obligation to monitor the information should be imposed on these providers (Article 7). In addition, the proposed Act imposes an obligation on the providers of intermediary services to enforce, as appropriate, orders issued by the relevant national

judicial or administrative authorities regarding illegal content (Article 8), and to furnish information (Article 9).

The proposed Act also contains a definition of illegal content, which stands for any information that, in itself or by its reference to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law (i.e., referring to content considered illegal under the provisions of media law, hate speech or copyright). A definition of dissemination to the public is also introduced, referring to making content available, at the request of the recipient of the service who provided the content, to a potentially unlimited number of third parties. The proposed Act defines the term "online platform" as a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another, and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this regulation. The term "content moderation" is considered to mean the activities undertaken by providers of intermediary services aimed at detecting, identifying, and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken which affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination or suspension of the recipient's account.

In compliance with the Polish standpoint on adopting the proposed Digital Services Act, the rule of the limited liability of online intermediaries (liability exceptions) should be upheld. The conditions to release the intermediary from liability should still include having no knowledge of the illegal character of the content, and removing or effectively preventing access to such content by the intermediary once it becomes aware of its illegal character. At the same time, the Digital Services Act should envisage penalties for those digital service providers which do not react appropriately to notices regarding illegal content. The requirement of the intermediary's neutrality towards illegal content as a prerequisite to being exempt from responsibility for users' content should be dropped, as it no longer matches the reality. Attention was rightfully drawn in that standpoint to the fact that, under the current digital-market conditions, the degree of activity in respect of content forms part of the service provision – for instance, in the context of the processing of personal information generated passively. The new solutions should combine a platforms' actions in identifying and removing illegal content with the protection against making them automatically responsible for the content disseminated via their services by third parties, including users. One of the solutions is to introduce the so-called "Good Samaritan" clause.

The introduction of the "Good Samaritan" rule referred to in recital 25 and Article 6 , under which the intermediary should not be punished for merely carrying out activities,

in good faith, aimed at removing illegal content, going beyond the obligations arising from the applicable Acts or regulations. What is more, intermediaries should be encouraged to do so. Nonetheless, it is worth making it even clearer that this rule does not exempt the intermediary from responsibilities arising from the obligation to react appropriately under the notice and action procedure, and as a result of receiving an order from the authorised body. The provisions must make it clear that the application of the "Good Samaritan" rule by a given intermediary is not automatically equivalent to its being exempt from any liability in any situation. The use of the proactive "Good Samaritan" measures by an intermediary should not, in principle, prevent it from using the exemption from liability, but it must not lead to a situation in which the intermediary invokes the "Good Samaritan" rule to evade liability, despite the fact that it takes other measures that would normally qualify under the liability principles of the proposed regulation. In line with recital 25: "In order to create legal certainty and not to discourage activities aimed at detecting, identifying and acting against illegal content that providers of intermediary services may undertake on a voluntary basis, it should be clarified that the mere fact that providers undertake such activities does not lead to the unavailability of the exemptions from liability set out in this Regulation, provided those activities are carried out in good faith and in a diligent manner. In addition, it is appropriate to clarify that the mere fact that those providers take measures, in good faith, to comply with the requirements of Union law, including those set out in this Regulation as regards the implementation of their terms and conditions, should not lead to the unavailability of those exemptions from liability. Therefore, any such activities and measures that a given provider may have taken should not be taken into account when determining whether the provider can rely on an exemption from liability, in particular as regards whether the provider provides its service neutrally and can therefore fall within the scope of the relevant provision, without this rule however implying that the provider can necessarily rely thereon."

The Digital Services Act proponent has also decided not to impose a general obligation on online intermediaries to monitor information posted by users. However, it is worth noting that the proponent has not waived the monitoring obligation in specific cases, though it has done so only in recital 26 and not in the main provisions of the regulation. According to that recital: Where possible, third parties affected by illegal content transmitted or stored online should attempt to resolve conflicts relating to such content without involving the providers of intermediary services in question. Recipients of the service should be held liable, where the applicable rules of Union and national law determining such liability so provide, for the illegal content that they provide and may disseminate through intermediary services. Where appropriate, other actors, such as group moderators in closed online environments, in particular in the case of large groups, should also help to avoid the spread of illegal content online, in accordance with the applicable law. Furthermore, where it is necessary to involve information society services providers, including providers of intermediary services, any requests or orders for such involvement should, as a general rule, be directed to the actor that has the technical and operational ability to act against specific items of illegal content, so as to prevent and

minimise any possible negative effects for the availability and accessibility of information that is not illegal content".

It is worth noting that, in line with recital 27, "services used for communications purposes, and the technical means of their delivery, have also evolved considerably, giving rise to online services such as Voice over IP, messaging services and web-based e-mail services, where the communication is delivered via an internet access service. Those services, too, can benefit from the exemptions from liability, to the extent that they qualify as mere conduit, caching or hosting service".

Other significant obligations arise from Articles 13 and 23 of the proposed Act, referring to transparency and reporting which should not violate business secrets, the confidentiality of commercial contracts, or user privacy. Transparency does not need to involve publicly disseminating detailed data and all the information required to the extent that they involve trade secrets or confidentiality. Such information and data should be provided only via reports addressed to supervisory bodies and the European Commission. The European Commission should ensure that the reporting rules are just, proportionate, and uniform, in all EU countries.

Under Regulation EU No. 524/2013 on online dispute resolution for consumer disputes, the right to use the online dispute resolution (ODR) platform was introduced. This is a European platform to be used by ADR (alternative dispute resolution) entities. Consumers must be notified of such a dispute resolution procedure, and the online store website must contain a link to the online platform.

In the process of the notifying of illegal content, it is important that the status of *trusted flagger* is awarded by the Digital Services Coordinator, which will not only enable the reliable verification of the entities applying for such a status, but will also facilitate eliminating entities intending to take measures in bad faith, while aligning the requirements with domestic needs, taking into consideration the public interest also dictated by public morality characteristic of a given community. It would seem advisable to enhance trusted flaggers in the context of the removing/blocking of the notified content by the platform. Notices submitted by trusted flaggers should be processed and decided on with priority in relation to notices submitted by ordinary users (as stipulated in Article 19 (1)), and they should be justified and monitored. In fact, Article 20 of the proposed Act authorises online platforms to take action against users and entities posting illegal content, or frequently submitting unjustified notices. These increase the legal certainty of platform operations, considering that a specific platform operation in such cases will not be based exclusively on the platform's terms and conditions which the users may challenge, but on explicit legal regulations.

The obligation for e-commerce platforms to identify the trustworthiness of business users (traders) will contribute to increasing users' confidence in online shopping, and to reducing the posting of illegal products, services, and content on these platforms, which

can make an important contribution to the identification efforts in the context of increased cybercrime. Data retention not envisaged in the Directive is important in the efforts to combat cybercrime. The retention of such data for two years for investigative purposes would enable the much more effective detection of crimes related to the provision of illegal products, content, and service.

8 Notifications and other mechanisms of intermediaries' activities

Intermediary services offering network infrastructure include internet access providers, domain name registries, hosting services such as cloud-based services and webhosting. Online platforms, such as online marketplaces, app stores, social networking and sharing platforms, and very large online platforms pose a particular risk when it comes to disseminating illegal and socially harmful content. The providers of hosting services are obliged to put mechanisms in place to allow any individual or entity to notify them of the presence on their service of illegal content. These mechanisms should be easy to access, user-friendly, and facilitate the submission of notices exclusively by electronic means. To that end, the providers should take the necessary measures to enable the submission of notices containing all of the following elements:

- an explanation of the reasons why the content is considered illegal;
- a clear indication of the electronic location of that information, in particular the exact URL or URLs, and, when necessary, additional information enabling the identification of the illegal content;
- the name and an electronic mail address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/UE;
- a statement confirming the good-faith belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete.

The Digital Services Act significantly enhances the mechanisms for illegal-content removal, and the efficient protection of fundamental internet users' rights, including the freedom of expression. It also increases the level of public control over the activities of online platforms, especially including those used by more than 10% of the EU population. Online platforms provide recipients of the service, for a period of at least six months, with access to an effective internal complaints handling system, which enables the complaints to be lodged electronically and free of charge, against decisions taken by the online platform on the basis that the information provided by the recipients is illegal content, or incompatible with its terms and conditions. This relates to online platforms which provide services to a large number of monthly active recipients (45 million or more), which is verified at least every six months by the Digital Services Coordinator.

It is worth adding that the service provider's liability is closely related to the status of knowledge of the unlawfulness of a given action (Gołaczyński, 2009 , Rączka, 2009). In the judgement of 18January 2011, I ACa 544/10 (LEX No. 736495), the Appellate Court

in Lublin adopted a standpoint that while the service provider is under no obligation to monitor its network, nor is it obliged to take measures to implement monitoring software, once it becomes aware of any infringement, or its illegal character, liability is to be undoubtedly considered to have arisen on the part of that provider.

The inclusion of the service provider's liability is not conditional on the exercising of diligence involving in particular the control of stored data. Article 15 of the APSEM stipulates that the entity which provides services specified in Articles 12–14 is not obliged to monitor the data referred to in these articles, which are transmitted, stored, or made available by that entity. Theoretically, this is because the suppliers of electronic services only provide an ICT base, and have no control over what is made available within the service. Thus, the issue of a service provider's lack of liability applies when they have no knowledge of the illegal content stored with them. However, in a different situation, when service providers become aware of such data (either on the basis of reliable information or as a result of official notification) – they are obliged to promptly block access to it. Service providers are then obliged to control the content of the stored data, which seems to be in conflict with the provision of Article 15 of the APSEM. Therefore, it may be argued that providers of electronic services, which include transmission, via the telecommunication network, of data supplied by the service recipient, or the provision of access to the telecommunication network, may be released from any liability towards third parties, and, in addition, that they are not under any statutory obligation to monitor the content of the service on an ongoing basis, in order to detect any illegal content (pursuant to Article 15 of the APSEM). However, as already indicated, this does not exclude the liability of instigators, helpers, or persons who knowingly take advantage of damage caused to others(Article 422 of the Civil Code).

9 The liability of video-sharing platform operators

Amendments to the Audiovisual Media Services Directive 2010/13/EU, by way of Directive 2018/1808, introduce certain obligations, including for a video-sharing platform operator with a registered office in the territory of a Member State, within the meaning of Article 3(1) of Directive 2000/31/EC. In compliance with Article 28a(3) of Directive 2010/13/EU, it is considered that a video-sharing platform operator has its registered office in the territory of a Member State for the purposes of Directive 2000/31/EC if a) it has a parent or subsidiary with a registered office in the territory of a Member State, or b) it is part of a group, and another unit of that group has its registered office in the territory of the Member State.

Member States prepare and keep updated a list of video-sharing platform operators with registered offices in their territories, or regarded as having a registered office in their territory, and identify the criteria on which their authority is based. Member States submit the list and its updated versions to the Commission. The Commission ensures that such lists are shared on a central database. In the case of any inconsistency between the lists, the Commission contacts Member States in order to seek a solution. The Commission

provides access to the database to national authorities or regulatory bodies (Article 28a(6) of Directive 2010/13/EU).

The appropriateness of measures is determined by considering the nature of the content, the damage it can do, and the attributes of the categories of people subject to protection, as well as endangered rights and legitimate interests, including the rights and interests of video-sharing platform operators and the users who create or publish content on such platforms, as well as the general public interest. The measures must be workable and proportional, taking into account the size of the video-sharing platform and the nature of the service provided. These measures lead neither to *ex ante* control nor to the filtering of content on posting it onto a platform if it runs contrary to Article 15 of Directive 2000/31/EC. For the purposes of the protection of minors, as referred to in Article 28b(1)(a) of Directive 2010/13/EU, the most harmful content is subject to the harshest access control measures. Member States may take measures aimed at blocking websites which either include or disseminate child pornography among internet users on their territories. These measures must be introduced based on a transparent procedure, and provide sufficient guarantees, especially in order to ensure that the blocking is limited to what is necessary and appropriate, and to inform users about the reason for blocking. The guarantees might also include the possibility to obtain court compensation.

The governmental draft Act on amending the Broadcasting Act and the Act on Cinematography (9th term of office, Sejm paper No. 1340) stipulated that, in compliance with Directive 2018/1808, video-sharing platform operators do not bear editorial responsibility. It should be assumed that the issue of exclusion of editorial responsibility applies only to the audiovisual content made available by the user, and not to any content available on the platform or the way it is organised.

In line with the definition provided in the Polish Broadcasting Act, "a video sharing platform is a service provided by electronic means, as part of business activity conducted in this area, the primary purpose of which (or of its severable part) is to provide the general public with programmes or user-generated videos, for informational, entertainment or educational purposes, for which the service provider has no editorial responsibility but it decides on the method of compilation, including automatically or by means of algorithms, in particular by displaying, tagging, and sequencing". This appears to be a regulation that, while limiting editorial responsibility, does not collide with other rules imposing the liability of online intermediaries contained in the Directive on copyright and related rights in the Digital Single Market and the draft Digital Services Act.

It is forbidden to place broadcasts, user-created videos or other transmissions on video sharing platforms (under the Broadcasting Act, "other transmission" means all kinds of transmissions that are not broadcasts or user-created videos; this notion, therefore, includes commercial communications as well as other types of undefined communications, such as non-commercial information from non-governmental organisations, the so called board broadcasts (still images displayed on a screen) or

a sequence of sounds without an accompanying image in a TV programme), which: 1) prejudice the physical, mental or moral development of minors, in particular those containing pornographic or gratuitously violent content, without effective technical protection; 2) containing incitement to violence or hatred towards a group of people due to gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, nationality, membership of a national minority, property, birth, disability, age or sexual orientation; 3) containing content that may facilitate the commission of a terrorist crime, pornographic content with the participation of minors, content inciting to insult a group of people or an individual due to his/her national, ethnic, racial, religious affiliation or lack of religious denomination.

With the aim of implementing the above obligations, the video-sharing platform provider: 1) sets up and implements effective technical safeguards, including parental control systems or other appropriate measures, in order to protect minors from access to broadcasts, user-generated videos or other transmissions that prejudice the physical, mental or moral development of minors, in particular those containing pornographic or gratuitously violent content; 2) enables users of a video sharing platform to qualify the broadcasts, user-generated videos or other transmissions posted by them, and to apply technical safeguards to the broadcasts, user-generated videos or other transmissions posted by them. The National Council, by way of a regulation, may set up detailed requirements to be met by effective technical safeguards or other appropriate measures, with a view to protecting minors from watching broadcasts, user-created videos or other transmissions, guided by the need to ensure the effective protection of minors from content harmful to them, taking into account technical possibilities, the degree of harmfulness of such broadcasts, user-created videos or other transmissions to minors in particular age categories and the specific nature of video-sharing platforms.

It is worth adding that on 20 June 2019 the European Parliament and the Council of the European Union adopted Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services. This regulation has been in force since 12 July 2020, introducing a number of legal regulations, crucial for the way internet services are provided. Their adoption was motivated by the desire to effect the inclusion of internet services into the same legal regime that applies to "traditional" audiovisual and telecommunications services. It defines the principles of the operation of online platforms and search engines. The need to adopt that regulation arose from the fact that the use of online intermediation services can be crucial for the commercial success of undertakings which use such services to reach consumers. In addition, online search engines can be important sources of internet traffic for undertakings which offer goods or services to consumers through websites. It was considered necessary to establish a set of mandatory rules at the Union level to ensure "a fair, predictable, sustainable and trusted online business environment within the internal market" (Wozniak, 2019:1-10).

An online search engine was defined as a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular

language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found, and the provider of an online search engine means any natural or legal person which provides, or which offers to provide, online search engines to consumers.

It should be stressed that Regulation 2019/1150 is applicable to business-to-business (B2B) relations: platforms which provide intermediary services and traders who sell goods or provide services thanks to that (*platform-to-business*, P2B, relations) (Article 2 of Directive 2019/1150). In contrast, Regulation 2019/1150 does not apply to business-to-consumer relations or to online payment services, nor to online advertising tools or online advertising exchanges (Article 1(3) of Regulation 2019/1150). It should be stressed that the online intermediation service must be an Information Society service, within the meaning of Article 1(1)(b) of Directive 2015/1535, that is to say, a service provided: 1) for remuneration, 2) at a distance, 3) by electronic means, and 4) at the individual request of a recipient of services. It is stressed in legal commentaries that services performed under *gig economy* will not exhibit such a character. The intermediation service was excluded from the definition of an Information Society service. This refers to situations where the intermediary service is merely ancillary to the main service, but without the online intermediary service the main service cannot be implemented. This is true, for instance, of Uber, BlaBlaCar or Airbnb, where the service provided is a composite service consisting of an electronically provided service, e.g., a service for matching passengers with drivers, and a non-electronically provided service, such as a transport service, where the primary service is transport and it is the transport that gives the service its economic meaning (Konarski, 2020:147-148). The obligations stipulated in Regulation 2019/1150 are binding on providers of online intermediation services. Under Article 2(3) of Regulation 2019/1150, a provider of online intermediation services means any natural or legal person which provides, or which offers to provide, online intermediation services to business users. These entities can be considered to include online auction sites (e.g., Allegro), online booking systems (e.g., Booking.com) social networking sites (e.g., Facebook), to the extent that they are used for business purposes, or search engines (Google) (Konarski, 2020:148). Among the most important obligations, which are primarily information obligations, imposed on providers of online intermediation services, the EU legislator has enumerated the following: 1) the obligation to ensure appropriate terms and conditions of use, and the procedure for amending them (Articles 3 and 8 of Regulation 2019/1150); 2) the obligation to set out the terms and conditions determining ranking (Article 5 of Regulation 2019/1150); 3) the obligation to provide a description of the technical and contractual access of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services (Article 9 of Regulation 2019/1150). Each Member State is to ensure the proper and effective enforcement of the Regulation. Member States shall lay down the provisions specifying the measures to be applied in the case of violations of Regulation 2019/1150

and shall ensure their enforcement. The measures envisaged must be effective, proportional and dissuasive.

10 Liability under Directive 2019/790 on Copyright on the Digital Single Market

Another example of regulation concerning the liability for content shared on the web is Directive 2001/29/EC, which introduces limitations on the liability for copyright breach. Article 5(5) of Directive 2001/29/EC creates the possibility to lay down exceptions connected with illegal use, and provided for in Article 5 (1)-(4) of Directive 2001/29/EC, including the exception for copies for private use as referred to in Article 5 (2)(b) of the Directive, dependent on fulfilling three conditions: 1) the exception is applied only in certain special cases, 2) does not breach the normal use of an original work of authorship, and 3) does not do unjustified damage to the reasonable interests of copyright subjects. The three conditions correspond, as follows from Recital No. 44 of Directive 2001/29/EC, to the international obligations of the Member States and the European Union, and more precisely, to the conditions relating to any limitations on copyright set out in Article 9(2) of the Berne Convention, commonly known as the "three-step test", repeated in Article 13 of TRIPS and in Article 10 of the WCT. This test shall also apply to the use of works on the web.

Notwithstanding the foregoing, the provision laid down in Article 17(4) of Directive 2019/790 on Copyright in the Digital Single Market remains a key measure, according to which, if not granted permission, online content-sharing service providers are liable for acts of public distribution not covered by permission, including making original works of authorship and other copyrighted items known to the public, unless they prove that: a) they have made every effort to obtain authorisation , and b) have made every effort – assuring the highest degree of professional care and conduct specific to the sector – to ensure the lack of access to respective original works of authorship and other copyrighted items, with reference to which rightholders have provided service providers with relevant and necessary information; and in every case c) acted without delay on receiving duly justified reservations from rightholders in order to block access to original works of authorship or other copyrighted items to which a reservation pertains, or to remove them from their websites, and made every effort to prevent their publication in the future in accordance with subparagraph b.

By evaluating whether a service provider fulfils the obligations referred to in Article 17(4) of Directive 2019/790, and in view of the principle of proportionality, one has to consider, among other things, a) the type, the audience, and scale of the services provided, and the kind of original works of authorship or other copyrighted items posted by the users of a service, and b) the accessibility of the appropriate and effective measures and their costs for service providers (Article 17(5) of Directive 2019/790). When the online content-sharing service providers are liable for public sharing, or for making content publicly known, on the terms set out in Directive 2019/790, Article 14(1) of Directive 2000/31/EC

should not apply to liability following from the provisions of this Directive concerning the use of protected content by online content-sharing service providers. That should not affect the application of Article 14(1) of Directive 2000/31/EC with reference to such service providers for purposes falling outside the scope of Directive 2019/790 (Recital 65 of Directive 2019/790). The same is true of the regulations regarding liability in the proposed Digital Services Act.

That regulation also introduces new rules for excluding liability of the service provider. This applies to information society services and excludes from the Directive such services as WhatsApp, even if they serve the same functions, for instance, as Facebook does. "[…] as well as providers of business-to-business cloud services and cloud services, which allow users to upload content for their own use, such as cyberlockers, or online marketplaces the main activity of which is online retail, and not giving access to copyright-protected content" (recital 62, clause 5, of Directive 2019/790). Such regulation excludes from the applicability of the Directive services such as Google Drive, Microsoft Drive and iCloud, despite the fact that they enable mutual content sharing. G. Spindler points out, however, that as a rule then the premise of access to a "large number" of works is not met (cf. Spindler, 2019:347, cited: Markiewicz, 2021:207) for infringement of exclusive rights to a work. An obligation was introduced to obtain authorisation from the rightholders of works and, where this is not obtained despite having made "all reasonable efforts, in accordance with high standards of professional diligence in the sector", to exclude liability, service providers are obliged to: a) prevent access to individual works and other protected subject-matter regarding which the rightholders submitted the relevant and necessary information to the service providers, and b) in each case duly notify the rightholders to block access to the exclusive subject-matter and to make every effort to prevent future posting.

Table 1: Liability of intermediaries

Legal act	Directive 2019/790	Directive 2018/1808	Digital Services Act
The obliged entity	The online content-sharing service provider means a provider of an information society service of which the main, or one of the main purposes, is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes.	The provider of a video-sharing platform service which means a service within the meaning of Articles 56 and 57 of the TFEU, when the primary purpose of that service (or of its severable part) is to provide the general public with broadcasts or user-generated videos, or both of these, for informational, entertainment or educational purposes – via the electronic communications network	The provider of an intermediary service which means one of the following services: a "mere conduit" service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;

		within the meaning of Article 2(a) of Directive 2002/21/EC – for which the video-sharing platform service provider has no editorial responsibility but it decides on the method of compilation, including automatically or by means of algorithms, in particular by displaying, tagging, and sequencing.	a "caching" service that consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request; a "hosting" service that consists of the storage of information provided by, and at the request of, a recipient of the service. An online platform means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation.
Scope of liability	If not granted permission, online content-sharing service providers are liable for acts of public distribution not covered by permission, including making original works of authorship and other copyrighted items known to	Video-sharing platform service providers are obliged to use appropriate measures in order to protect: a) minors against broadcasts, user-created videos, and audiovisual commercial	Mere conduit, caching, hosting Hosting service providers shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of

	the public, unless they prove that: a) they have made every effort to obtain permission, b) have made every effort – assuring the highest degree of professional care and conduct specific to the sector – to ensure the lack of access to respective original works of authorship and other copyrighted items, with reference to which rightholders have provided service providers with relevant and necessary information; and in every case c) acted without delay on receiving duly justified reservations from rightholders in order to block access to original works of authorship or other copyrighted items to which a reservation pertains, or to remove them from their websites, and made every effort to prevent their publication in the future in accordance with subparagraph b.	communications which could be harmful to their physical, mental, or moral development – in accordance with Article 6a(1) of Directive 2018/1808; b) the general audience against broadcasts, user-created videos, and audiovisual commercial communications which incite violence or hatred towards a group of people or a member of a group, for the reasons referred to in Article 21 of the CFR; c) the general audience against broadcasts, user-created videos, and audiovisual commercial communications which include content whose distribution is an act, qualifies as a crime under EU law, i.e., public incitement to commit a terrorist crime, as defined in Article 5 of Directive 2017/541, a crime connected with child pornography, as defined in Article 5(4) of Directive 2011/92/EU, and a crime motivated by racism and/or xenophobia, as defined in Article 1 of Framework Decision 2008/913/JHA. Member States may subject video-sharing platform providers to more detailed or stricter measures than those referred to in Article 28b(3) of Directive 2010/13/EU. In adopting such measures, Member States shall comply with the requirements set out in applicable Union law, such	information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means.

		as those set out in Articles 12–15 of Directive 2000/31/EC or Article 25 of Directive 2011/93/EU	
Filtering	Yes, but this results from the scope of liability and not directly from the provision.	Member States should ensure that all video-sharing platform operators should apply these kinds of measures in their jurisdictions. The measures must be workable and proportional, taking into account the size of the video-sharing platform and the nature of the service provided. These measures shall lead neither to *ex-ante* control nor to the filtering of content on posting it onto a platform if it runs contrary to Article 15 of Directive 2000/31/EC. For the purposes of the protection of minors, as referred to in Article 28b (1)(a) of Directive 2010/13/EU, the most harmful content is subject to the harshest access control measures such as: establishing and operating multiple user verification systems for video-sharing platforms to detect content which could be harmful to the physical, mental, or moral development of minors; establishing and operating easy-to-use systems enabling video-sharing platform users to assess the content referred to in Article 28b(1) of Directive 2010/13/EU; – ensuring parental control systems subject to end-user control to detect content which could be harmful to	Content moderation means the activities undertaken by providers of intermediary services aimed at detecting, identifying, and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken which affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination or suspension of the recipient's account. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review. It shall be set out in clear and unambiguous

		the physical, mental, or moral development of minors.	language and shall be publicly available in an easily accessible format. Such information shall be formulated in a clear and unambiguous manner and shall be provided to the public in an easily accessible format.
Blocking	The provider is obliged to block access to a given file or remove it from its websites by way of: 1) monitoring the content available on a given platform, and 2) the file containing an illegally located work being detected by the rightholders, and 3) monitoring the platform content after removing the file concerned.	None	Providers of intermediary services shall, upon the receipt of an order to act against a specific item of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union or national law, in conformity with Union law, inform the authority issuing the order of the effect given to the orders, without undue delay, specifying the action taken and the moment when the action was taken. Online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content. Online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the processing of notices and complaints submitted through the notice and action mechanisms and internal complaints-handling systems referred to in Articles 14 and 17 of the

			DSA, respectively, by individuals or entities or by complainants that frequently submit notices or complaints that are manifestly unfounded.
Right of appeal	An effective complaints and redress mechanism available to users of their services in the event of disputes concerning the blocking of access to or removal of original works of authorship or other copyrighted items	Establishing and operating systems through which video-sharing platform providers explain to users of video-sharing platforms what effect has been given to the reporting and flagging. Establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints to the video-sharing platform provider in relation to the implementation of the measures referred to in points (d) to (h) of Article 28b(3) of Directive 2010/13/UE. Member States shall ensure that out-of-court redress mechanisms are available for the settlement of disputes between users and video-sharing platform providers relating to the application of Article 28b (1) and (3) of Directive 2010/13/EU. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law. Member States shall ensure that users can assert their rights before a court in relation to video-sharing platform providers pursuant to Article 28b (1)	Online platforms shall provide recipients of the service, for a period of at least six months following the decision referred to in this paragraph, access to an effective internal complaint-handling system, which enables complaints to be lodged electronically and free of charge, against the following decisions taken by the online platform on the grounds that the information provided by the recipients is illegal content or incompatible with its terms and conditions: a) decisions to remove or disable access to the information; b) decisions to suspend or terminate the provision of the service, in whole or in part, to the recipients; c) decisions to suspend or terminate the recipients' account. Recipients of the service addressed by the decisions referred to in Article 17(1) of the Digital Services Act shall be entitled to select any out-of-court dispute that has been certified in accordance with Article 18(2) of the Digital Services Act in order to resolve disputes relating to those decisions, including complaints that

		and (3) of Directive 2010/13/EU.	could not be resolved by means of the internal complaint-handling system referred to in that Article. Online platforms shall engage, in good faith, with the body selected with a view to resolving the dispute and shall be bound by the decision taken by the body.

Source: the author.

11 Summary

The examples presented above prove the principle that, in each case, the liability of each entity is different, depending on whether it provides the services referred to in the Act on the Provision of Services by Electronic Means, or whether it is a broadcaster or a publisher. As a result of technological and economic convergence, the same entity may perform very different functions, and it is not determined what its status will be, so the scope of its liability is not conclusively determined. The situation calls for appropriate regulations, with the reservation that there is a need to synchronise issues at each stage of legislative activity. It is an element indispensable to creating a coherent system of legislative frameworks facilitating the growth of the digital-services sector, taking into account the basic principles of liability for distributing content. The notice and take-down procedure is still applied in many countries. Directive 2000/31/EC on Electronic Commerce also stipulates that service providers are obligated to respond to content inconsistent with the law, having received a notice (complaint) about the fact. (For more information about digital content-related crime, see K. Chałubińska-Jentkiewicz, 2019:283, especially the chapter on cybercrime [Cyberprzestępczość, wybrane zagadnienia]). Of great importance for the appropriate and effective operation of the notification procedure are special websites appointed for such purpose, by means of which end users may report any illegal content they come across on the internet (Siwicki, 2011:258 et seq.).

Under the present conditions of digital platform development, one expects that the intermediaries of online services should be held to account for content and to protect users, especially those whose rights are being infringed, against certain kinds of illegal content available online. In response to those concerns, in order to ensure greater certainty in the law, and to prevent the fragmentation of the internal market, one needs to consider introducing a framework for reporting mechanisms and removing illegal content (the notice and action procedure) in the territory of the whole EU, covering measures proportional to the character and impact of the mechanisms of damage, to make it possible for unambiguously illegal content to be promptly and effectively removed. The aim is to

minimise potential damage, and to provide a mechanism for securing removed content, if necessary, to prevent, detect, or conduct an investigation in connection with a crime, and to prosecute cybercrime.

It will be necessary, however, to ensure the right balance between the interests and expectations of those who report illegal content which should be removed and those who publish content, making it possible for them to object to its removal (counter-notice). A new regulation must guarantee for the intermediaries of internet services an appropriate level of legal certainty, and improve coordination and cooperation among national authorities and with the European Commission. However, the most important are the interests of network users, the recipients of digital services, who need transparency and a quick reaction. One may not, at the same time, reject internet users' rights to free speech and the right to information.

Another issue worth considering is the character of global competition and respect for consumers' rights. The rigorous rules of competition and open markets have made the EU one of the richest and most competitive economies in the world. The European Commission said that it "is presently analysing the effectiveness of the way in which the relevant provisions of law are applied, for example, to the measures of the protection of competition, and is also evaluating and reviewing these very provisions in order to ensure that they fulfil their objectives in view of the current challenges posed by digital technologies and environmental protection" (Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Shaping Europe's digital future, COM(2020) 67 final, point 2B). Certainly, new provisions are necessary so that they can be adapted to the new conditions of the digital environment. On the one hand, legal provisions which are too rigorous are not conducive to the growth of the market, which creates the risk of evading regulations and registering one's activities in a territory which is less legally restrictive. On the other hand, regulation is required in the case of risks in which only a legal norm is capable of ensuring the socially expected protection of an individual and the state.

References:

Barta, J. & Markiewicz, R. (1998) *Internet a prawo* (Kraków: Wydawnictwo Universitas).

Chałubińska-Jentkiewicz, K., Nowikowska, M. & Wąsowski, K. (2020) *Media w erze cyfrowej. Wyzwania i zagrożenia* (Warszawa: Wolters Kluwer).

Chałubińska-Jentkiewicz, K. (2019) *Cyberodpowiedzialność* (Toruń: Wydawnictwo Adam Marszałek).

Garton Ash, T. (2018) *Wolne słowo. Dziesięć zasad dla połączonego świata* (Kraków: Wydawnictwo Znak).

Gęsicka, D.K. (2014) *Wyłączenie odpowiedzialności cywilnoprawnej dostawców usług sieciowych za treści użytkowników* (Warszawa: Wolters Kluwer).

Gołaczyński, J. (ed.) (2009) *Ustawa o świadczenie usług drogą elektroniczną* (Warszawa: Woleters Kluwer).

Konarski, X (2020) Nowe obowiązki dostawców usług internetowych w prawie polskim i Unii Europejskiej, *Monitor Prawniczy*, 2020(20), pp. 147 - 153.

Litwiński, P. (2004) Świadczenie usług drogą elektroniczną, In: Podrecki, P. (ed.) *Prawo Internetu* (Warszawa: Wydawnictwo Prawnicze LexisNexis), pp. 166-245.

Markiewicz, R. (2021) *Prawo autorskie na jednolitym rynku cyfrowym. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790* (Warszawa: Wolters Kluwer).

Rączka, G. (2009) Prawne zagadnienia hostingu, *Przegląd Prawa Handlowego*, 2009(4), pp. 31-37.

Siwicki, M. (2011) *Nielegalna i szkodliwa treść w internecie* (Warszawa: Wolters Kluwer).

Spindler, G. (2019) The Liability system of ART. 17 DSMD and national implementation – contravening prohibition of general monitoring duties, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 10(3), pp. 344-374.

Woźniak, M. (2019) Antykonkurencyjne praktyki w relacjach między przedsiębiorcami: uwagi na tle nowego rozporządzenia P2B, *Zeszyt Naukowy.pl. Wyższa Szkoła Zarządzania i Bankowości w Krakowie,* (52), pp. 1-10.

Zieliński, M. (2013) *Odpowiedzialność deliktowa pośredniczących dostawców internetowych. Analiza prawno porównawcza* (Warszawa: Wolters Kluwer).