Chapter I

Security Risks and Public Risk Perception Associated with Digital Media

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ

Abstract The media system is the simplest reflection of the social and political situation in a country. The media are also important for state policy, for understanding the value of the public interest. This is especially the case when, when the media are analyzed in the context of their paternalistic role, i.e. their public mission in terms of educating the public, active in public life, according to a sense of axiology and national identity, etc. This is all the more important because in the media market, significant even revolutionary changes are taking place, leading to its liberalization. This is creating the conditions for the development of an alternative media system based on the principles of competition and the provision of a so-called digital service. At the same time, media rules are being unified on a European scale, which particularly concerns new technological conditions and the protection of market rules. In this area, it is obvious and desirable to create completely new solutions enabling the exchange of experience and the preservation of basic requirements defined at EU level. Therefore, the creation of a strengthened organizational system is needed, but without interfering in the regulatory area of the EU Member States. The digital media environment is subject to obvious changes, but it is still the state that plays an important role as a regulator of media reality. At the core of the functioning of a democratic state under the rule of law is freedom of expression. Therefore, on the one hand, the media are a check on the activities of the authorities, but on the other hand, they are also subject to such supervision. It is important to emphasize the position that the specific role the media play in the state and society needs to be assessed from the point of view of the overriding good, which is the public interest in national terms.

Keywords: • digital content • social media • public interest • service users

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Associate Professor, Kozminski University, College of Law, Jagiellonska 57/59, 03-301 Warszawa, Poland, e-mail: kasiachalubinska@gmail.com, ORCID: 0000-0003-0188-5704.

https://doi.org/10.4335/2024.2.1 ISBN 978-961-7124-25-5 (PDF)
Available online at http://www.lex-localis.press.

If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed and, in the next place, oblige it to control itself.

J. Madison

1 Introductory remarks

Answers to the questions concerning the methods of applying the law, as an instrument to influence the market and public governance, should be sought for regulation purposes and for redefining public interest objectives. The primary purpose of digitisation is to secure the development of society in the digital consumption era. Due to the passage of time and the development of new transfer techniques, the digital resources meeting the adopted standards related to their legal sharing are dramatically diminishing. Digital content constitutes a source of knowledge, inspiration, and skills for present and future generations. The underlying public tasks related to digitisation include organising digital resources and managing them modernly. The present and future duties of entities and participants in the market for digital services in the digital world need to be normatively established. This requires infrastructure owners to cooperate with owners of digital resources and the respective public institutions of e-administration.

Another significant objective is to provide Internet access to digital content. Since Internet technologies have been popularised, and more and more materials are being shared via the Internet, it is becoming necessary to determine which priorities should be adopted to lay down the principles of access to resources after the digitisation process. Should it be a common public service? Or should access be limited to information security (classified information, personal data, copyright, etc.) or to private or economic interest?

The questions relating to public governance in cyberspace also apply to the matter of implementing the directives on the reuse of information from the public sector. Encouraging people to reuse digital content constituting the public domain is obvious. However, the reuse of digital resources, e.g., by the private sector, raises many problematic issues, such as intellectual property rights, data protection, policy concerning the collection of fees, and the market competitive balance between public and private services.

The management of digital content-sharing processes changes due to the increasing commitment of various social groups to the functioning of a modern information society. One should bear in mind that the contemporary digital resources shared with the use of digital media, which were often developed from the traditional ones, must be a reliable and legal source of knowledge. At the level of the contemporary development of the digital society, it is necessary to lay down the rules for managing digital resources at all

stages of digital content circulation. Just as public institutions must participate in the management of market processes at the level of both the government and the local-government administration sectors, it seems that they should do so in both the technological aspect and through the development of new strategies and planning. The last matter to be resolved is the significance of the legal principle. According to R. Cooter and T. Ulen, the economic analysis of law can be divided into positive (dealing with evaluating the effects of particular regulations regarding their economic efficiency) and normative (providing broadly-construed recommendations and postulates regarding legislative activity). The case described by R. Cooter and T. Ulen, in their book titled *Law and Economics*, can serve as an exemplary solution (Cooter, Ulen 2011: 166). Referring to the problem of the future protection of copyright in cyberspace, the authors provide several solutions. It might be collective management, the so-called celestial jukebox, under which every digital information user will pay royalties to a central clearing house managing the copyright. Then, copyright will become the dominant law of the digital age. Another solution is "digital libertarianism", in which technical protection through cheap encrypting will be more efficient than the legal protection of intellectual property, and copyright law will die out because technology will make the law unnecessary. Perhaps this is the fate of many other regulations in the modern world, as we still do not know whether new laws respond to new mechanisms or contrariwise (Cooter, Ulen, 2011: 166–167).

Driven by digital technology advancements, the functioning of the European media sector in the digital age is generating increased consumer demand and globalisation. These processes are posing new challenges for the regulators. Digitisation is defined as the conversion of a signal (e.g., processed sound, images, and data) from analogue into digital form through analogue-digital processing. Also, it means converting analogue format into digital (binary) format, which can be stored in computer memory. The term *digitisation* stems from the word *digit*, which originated from the Latin *digitus* (finger, toe, counting fingers). On 3 October 1997, the European Commission issued the already inapplicable Communication No. 623 – the Green Paper on the convergence of the telecommunications, media and information technology sectors, and the implications for regulation (the Green Paper on the convergence of the telecommunications, media and information technology sectors, and the implications for regulation towards an information society approach, COM(97) 623 (non-applicable version).

In the Green Paper, the Commission highlighted that computer technology played a key role in content creation and broadcasting. The digital media field has since, however, undergone enormous change, with content – and, more specifically, digital content – being now created by all users in the digital world.

Due to its widespread accessibility and social impact, the Internet creates the most extensive opportunities for everyone to participate in political and cultural life by creating and sharing digital content. The development of the information society is accompanied

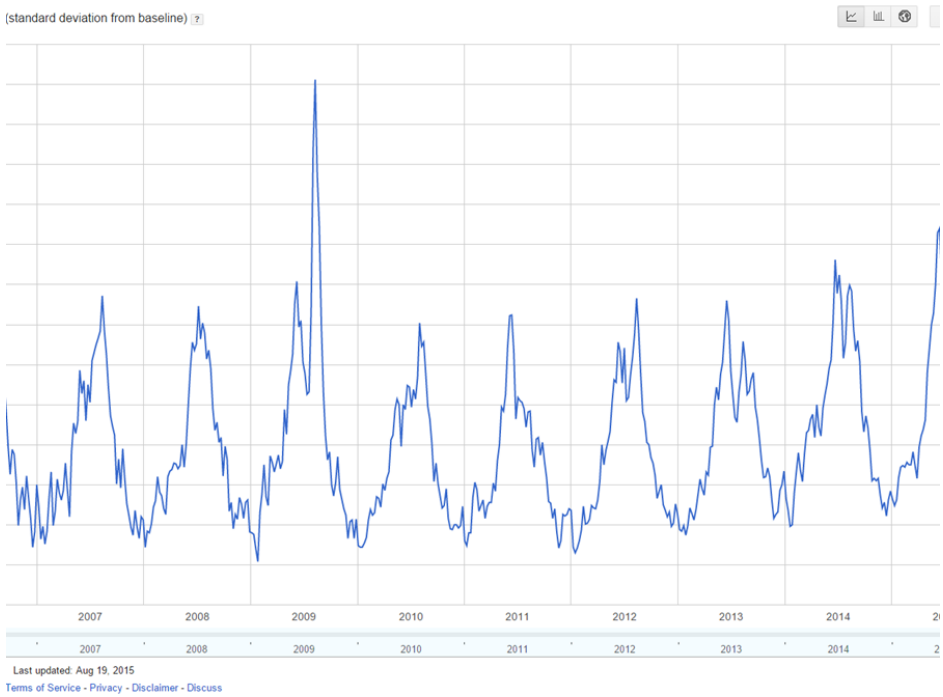
by civilisational as well as economic and cultural development. Mass communication is becoming a source of knowledge about the world, driving the emergence of a mass and global society. Each day, the Google search engine responds to three billion queries, and all of them are archived. Big data poses a challenge to outer interactions with the world (a free online service of Google developed to translate texts, text files, websites, speech, pictures, and videos into 100 languages in real-time. While a text is entered, the service translates it in real-time. If a single word is put in, Google Translate works like a dictionary, usually providing from several to a dozen-odd suggested meanings. Google Translate is used by 200 million people daily. Since September 2016, Google Translate has had a new engine, GNMT, Google Neural Machine Translation – based on recurrent neuronal networks. The program now translates whole sentences (whereas earlier it translated single words), significantly improving the quality of the target-language text. It has supported the Polish language since March 2017).

GNMT improves translation quality because the system learns from millions of available examples. By using this broader context, it can find the most accurate translation. It then processes and adapts it to more "human" speech with the correct grammar. By using all these data, we can identify links and details which would otherwise be lost in the sea of information. The most interesting information is that which deviates from the norm, and the only way to identify it is by comparing vast numbers of transactions. For example, the unauthorised use of credit cards is detected by searching for anomalies. As the amounts of data grow, so do inaccuracies since large datasets always contain incorrect figures and distorted information. Yet, big data compensates for this lack of order.

Society benefits from big data not because of the faster processors or improved algorithms but because of the larger quantities of data. It is not causality but correlations that will be searched for. Around seven billion stocks trade hands on the US stock exchange daily. Approximately two-thirds of all these transactions are initiated by computer algorithms, which process vast amounts of data to bring profit at an acceptable risk. Facebook processes 10 million new pictures every hour, and 800 million YouTube users upload an hour of new videos every second. Each year, the volume of messages on Twitter is growing by about 200%. Big data relies on prediction. Amazon can recommend books to users, Google can display the requested website, and Facebook knows what its users like, while LinkedIn can guess whom users know or might know. Twitter, LinkedIn, and Facebook create "sociograms" of their users to identify their preferences (Microsoft acquired Farecast in 2008. It was an online booking portal publishing predictions on the best times to buy airline tickets. Farecast was founded by the American scientist Oren Etizioni in 20003. In 2007, it recorded more than 175 billion views of airline tickets. Farecast's data monitoring team used airline ticket price observations to develop algorithms predicting future price movements. In May 2008, Microsoft integrated Farecast's website with the Live Search engine to create the Live Search Farecast program, registering it in June 2009 as Bring Travel as part of the work on developing new search mechanics).

Thanks to large datasets, decisions can be made not by humans but by machines. There is a growing awareness in Poland that efforts should be made to support digital integration. The problem, however, lies in the lack of a systemic approach to digitisation and the lack of a coordinated approach to digitisation initiatives, including regulatory ones, causing the duplication of efforts and the underperformance of measures. The media sector has a key role to play in developing European citizenship, as it is one of the core means of communicating the common, fundamental social and cultural values of the Union to European communities, particularly young people. Digitisation aims to secure these in the form of high-quality digital copies and also to provide users with the broadest possible access to national heritage resources by creating online archives, library resources, and digital repositories. Digitisation and network technologies are essential drivers of economic and social development. Importantly, these phenomena are not only the domain of the public sector. Rather, it is private resources which largely constitute the most valuable sources of knowledge about their owners, holders, and users. And this, in the current age of profiling for marketing and other purposes, represents the most valuable marketable good. Digital content protection objectives can be achieved only by ensuring that digital initiatives, thus far largely dispersed, are coordinated in terms of creating resources, providing them with long-term protection, and establishing fair and transparent conditions for their sharing. Social media are essential vehicles for sharing content on the Internet.

Figure 1: Google Flu Trends Data



Google Flu Trends is an online service designed to estimate the number of flu infections in more than 25 countries. By linking Google search queries, Google wanted to make accurate projections about the spread of influenza. The project was launched in 2008 by Google.org to prevent the spread of flu epidemics. Google Flu Trends is no longer publishing current estimates. Historical data are still available, while current information is provided only for research purposes.

2 The impact of social media on the public sphere

Addiction to social media has been an ever-growing concern as the number of users and smartphone owners continues to rise, especially among young people. Yet, it is not only millennials who are exposed to Internet-related threats. Older people also spend more and more time online, including on social media.

Research shows that social media abuse reduces psychological well-being and satisfaction with one's appearance. To some extent, it also influences the way we see the world. Prolonged exposure to social media can also lead to eating disorders, sleeping

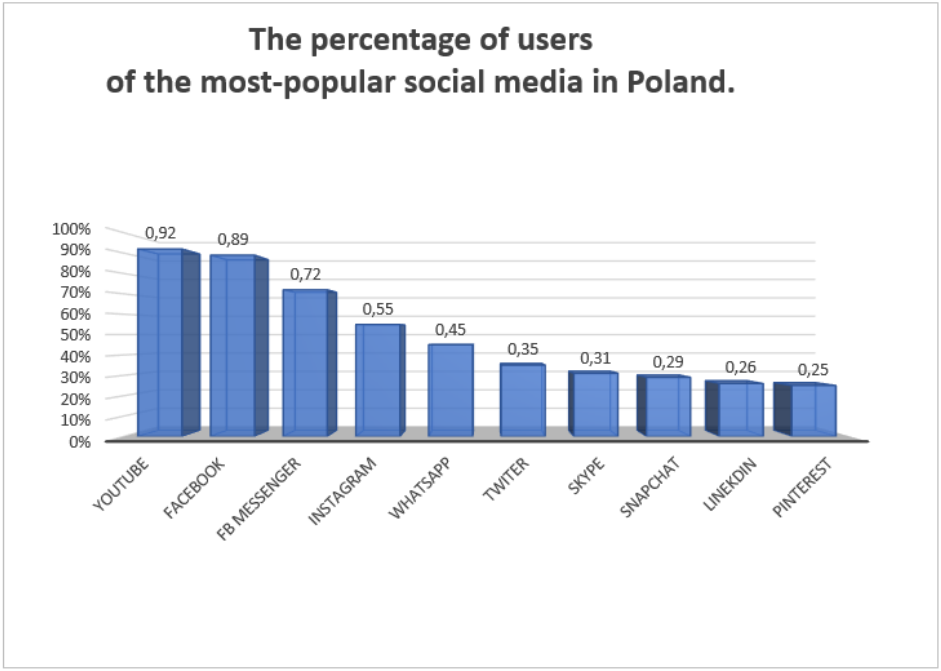
problems, and even fits of aggression. Fortunately, it is increasingly the subject of social and scientific debate, raising awareness about these critical and direct threats to Internet users. According to S. Galloway, "It's easy to be sceptical about Facebook, especially with all of the self-promotion, fake news, and groupthink spread on the platform. But it's also hard to deny it nurtures relationships, even love. And there is evidence that these connections make us happier" (Galloway, 2018:130). This is clearly the case with my retired father, who has now connected with his schoolmates with whom he had had no contact throughout his professional and private lives. As well as reconnecting with old acquaintances, Facebook allowed him to discover new interests, and even the theft of his identity and the blocking of his account did not stop him from surfing Facebook.

However, apart from the defined threat involving additions from the Internet, there are other issues with potentially much broader implications.

Although browsing social services is widely abused (mainly out of boredom), it can also be used more consciously, including for business purposes. Social media are excellent tools to find varied information and to get consumer feedback. This is well exemplified by Facebook groups, which focus on a single, often niche, topic or issue. By visiting these groups, we can get lots of essential information on a subject of interest to us or talk to people who seem to have similar interests (www.whysosocial.pl).

In addition to functional, strictly social advantages afforded by such services, social media are currently used as vehicles for influencing public opinion. It is not uncommon for election campaigns to rely substantially on the Internet to manipulate facts to undermine other candidates. This has become commonplace now, with social media being sources of information with questionable reliability. Furthermore, users are inundated with product advertising campaigns and sponsored messages designed to match their behavioural patterns, habits, and individual preferences. All these elements of being part of the Internet community generate a sense of chaos and uncertainty about the rules governing the digital market.

Chart 1: The most popular social media in Poland



Source: Based on the #Digital2020 report,https://mobirank.pl/2020/02/23/digital-mobile-i-social-media-w-polsce-w-styczniu-2020-roku/ (10/07/2020).

According to Digital2020 (www.datareportal.com), as of January 2020, there were more than 19 million social media users in Poland. YouTube, the video-sharing platform operator, was the leading social media site in Poland, with 92% of Internet users in Poland accessing the resources of this online service. YouTube was followed by Facebook, with 89% of Internet users. At 72%, the third place was taken by Messenger, followed by Instagram (55%) and WhatsApp (45%). Those further down the chart are clearly less popular, with fewer than 50% of Internet users reporting their presence on these services.

Social media are now undoubtedly the largest source of information and the leading space for processing digital content. On the one hand, such media expand access to sources of information and, on the other, the globalisation and availability of digital resources of various kinds and values cause users to be closed in "information bubbles", in which they function within a restricted circle of personalised information. This creates a kind of separation from other content outside the scope of the user's interests. The reason is that, as marketing and advertising algorithms inundate users with advertisements of the product they are looking for, the algorithms used in content searching match the content

to the interests and the users' specific needs. These activities are mainly self-regulated through the terms of use of individual social media. For instance, in Facebook's Terms of Service, the need for personalisation is expressed as a suggestion (www.facebook.com/legal/terms). It should be added that it is enough to talk about or express any interest using a smartphone, or "near a smartphone", for the mobile device to singly decipher and classify user interests as part of profiling. Nearly every movement, voice, and sign of interest plays a role. Not to mention geolocation-based analyses. A crucial task of social media is to attract the audience's attention. YouTube is an example of this, as it introduced a simple, and yet effective, method of attracting audiences merely by playing videos with related subjects one after another. Netflix, a provider of audiovisual on-demand services, adopted a similar approach of suggesting related content after watching a video or playing another episode in a series. User attention is the primary objective of Snapchat, the major messaging app used by teenagers. It should be noted, however, that whilst it is more of a communication aid for adults, for underage users, the app constitutes a *centre* for communication. Snapchat has introduced "Snapstreaks" – an update which tracks the number of days during which two users exchange "snaps" daily. Snaps are not necessarily regular conversations but pictures of a street, wall, or other objects without specific information. Still, data obtained from content shared in this way are used for analysis and drawing conclusions. Data are employed to analyse information about users and their environments. "A privacy advocate's nightmare is a marketer's nirvana. The open nature of Facebook, coupled with the younger generation's belief that 'to be is to share', has resulted in a data set and targeting tools that make grocery store scanners, focus groups, panels, and surveys look like a cross between smoke signals and semaphore (...). When you have the Facebook app open on your phone in the United States, Facebook is listening… and analysing" (Galloway, 2018:131).

With such vast amounts of data regarding users, which are available to them, media companies can not only reap substantial profits but also, in a sense, create a digital reality. As an example – consider the "PizzaGate" conspiracy theory, according to which officials affiliated with the former US presidential couple and members of the Democratic Party, including members of the Washington elite, were involved in a paedophilia ring. The central premise on which online investigators based their claims was that a paedophilia ring had an affiliation with a pizzeria. "Cheese pizza" is one of the English expressions used to refer to child pornography, its abbreviation "CP" also being understood as "Child Porn". The scandal erupted in early November 2016 when WikiLeaks published another batch of emails by John Podesta, Hillary Clinton's campaign manager. Unidentified perpetrators hacked into Podesta's account. Then, amidst the tension surrounding the upcoming elections, they stole data on email correspondence. However, a new batch of the campaign manager's emails was published by a user of the popular Internet forum, 4chan. The post implied that, this time, the correspondence contained major revelations, purporting that Podesta was a member of a paedophilia ring. This led to a proliferation of analyses on Reddit, and the "PizzaGate" subreddit was created for all topics around "PizzaGate", bringing together around 22,000 followers, including 1,500 active users.

This scandal was part of a broader trend of fake news, often craftily fabricated facts and lies. The very place these discussions were held was suspicious, with 4chan and Reddit being notorious for Internet memes. People came to believe that the owner of the Comet Ping Pong pizzeria was involved in child trafficking and molestation. They also claimed that Hillary Clinton and John Podesta were part of the conspiracy. As Comet Ping Pong began receiving telephone threats, fiction became reality. These attacks were initially only unsavoury jokes about "a special pizza" or other absurd names used to allude to paedophilia. Eventually, though, they became actual threats: "We'll kill you all", "We know where you live, you better kill yourself". One of the threats said "I'll go the restaurant with a rifle and kill you all, I'll rip your guts out and watch you die like an animal". The culminating point came when Edgar Maddison Welch from North Carolina arrived at the pizzeria, believing that children were being imprisoned and raped in the establishment's basement. A father of two, Edgar was convinced that he was on a rescue mission. One Sunday afternoon, when the pizzeria was full of families with children, the man entered the restaurant. He was armed and screamed at the people, telling them to leave the building. Then, he proceeded to search it. After rummaging through the entire establishment, he found only a locked door, which he shot open. The door led to the backrooms. Here, he saw a small sanitary room instead of a basement with children imprisoned. Edgar Maddison Welch was ready to go to jail or die because of false, misleading information (Rossi, 2020:498). The PizzaGate story demonstrates the magnitude of the impact that content created on social media can have on Internet users.

Hence, it should be assumed that the authenticity of digital content online depends not on accuracy, truthfulness or reliability. It is rather a matter of user reactions, such as 'likes' and reposting. These also create digital content which defines social preferences. In addition, such behaviour is used for political and criminal purposes. Generally speaking, it can be assumed that social media initially became a self-sufficient form of communication for organising protests and enabling activists and citizens to communicate their specific needs (e.g., through tweets calling for blood donors). Mainstream journalists realised that social media users had access to information or voided materials to which they had no access. This was due, for instance, to bans imposed by media organisations or Internet and telecommunication network blockades. Meanwhile, social media users were checking content for legitimacy and accuracy, aware that social media are not regulated in this respect (Bebawi, Bossio, 2014:135).

3 The responsibilities of digital content providers

The business of digital content providers consists of making content available through information and communication systems. This category is highly diverse. It includes not only specialised institutions but also end users. The latter group is particularly active due to the growing popularity of user-generated sites (or user-generated content – UGC).

Due to the active form of online operations, content providers seem to bear direct liability for any breaches caused by such operations. In Poland's legal system, content providers are directly liable for infringements of third-party rights. As noted by J. Barta and R. Markiewicz, controversies arose around attempts at qualifying the act of making works available on computer networks. Ultimately, this was qualified as a new field of exploitation, i.e., making a work available in a way that it could be accessed by anyone at any time and place they choose (Barta, Markiewicz, 2001: 228). This issue was highly relevant for ICT networks, whose function was based on interactivity. As a result of digital processes, users can modify and share content without problems. The concept emerged of *sui generis* protection for the rights of online content producers or providers. It was discussed at the Association Littéraire et Artistique Internationale (ALAI) congress in 1996, with attempts to formulate a construct allowing producers to claim protection against third parties. Among others, consideration was given to affording them the status of moral rights or quasi-moral rights, with the caveat that they might not have limited the moral rights of content creators (Dietz, 1997; as cited in Gęsicka, 2014:290). According to J. Barta and R. Markiewicz, the construction of these rights is similar not to moral rights but to the economic rights vested in authors (Barta, Markiewicz, 2001: 228). It was this core objective, primarily economic, that these entities had in mind, bringing these rights closer to related rights.

As regards other infringements, direct liability was also assigned to content providers. Therefore, they were no longer exempt from liability, which used to be restricted to the suppliers of electronic services. Technological changes influenced the scope of liability for illegal acts in cyberspace. Also, new rules on the limitation of this liability were introduced. In European law, the liability of online service providers is regulated by Directive 2000/31/EC, which lays down the rules governing the liability of digital content intermediaries. The Directive contains provisions on the most popular online services, i.e., mere conduit, caching and hosting. It should be noted that the European regulation follows the horizontal model. This means that the exemptions it provides apply to any legal liability, including civil, criminal, and administrative liability. The Electronic Commerce Directive lays down the rules for excluding liability at the maximum level. Consequently, individual Member States may decide to impose less strict solutions. Similar liability rules are laid down in the draft Regulation of the European Parliament and of the Council on a Single Market for Digital Services (the Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final.

The provisions of the Electronic Commerce Directive were implemented into Polish law by Articles 12–15 of the APSEM. Under Article 12 of this Act, relating to the mere-conduit service, "no liability for the provided information shall be assigned to those transmitting data who 1) have not initiated the transmission; 2) have not chosen the recipient of the data; and 3) do not remove or modify the data transmitted. The exclusion of liability referred to in paragraph 1 extends also to the automated short-term indirect storage of the transmitted data, provided that this is required only to complete the

transmission and that data are not stored longer than necessary in normal circumstances for completing the transmission (caching)" (Article 1(2) of the APSEM).

Caching – etymologically deriving from the French word *cacher*, meaning to hide or conceal – is an automated process of creating temporary copies of digital data to allow greater data accessibility for more frequent use. Caching is permissible as an exception to the right to reproduce a work under Article 5(1) of Directive 2001/29/EC. This provision establishes the rule according to which specific acts of temporary reproduction, which are transient or incidental reproductions, form an integral and essential part of a technological process and are carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or the lawful use of a work or other subject-matter, to be made.

In the case of the caching service, the waiving of liability for storing data applies to entities which transmit such data and ensure their automated and short-term indirect provision to help other entities re-access them on request, but which 1) do not remove or modify such data; 2) use recognised and customary IT techniques defining the technical parameters of data access and updating; and 3) do not interrupt the use of recognised and customary IT techniques to collect information about the use of the data gathered (Article 13(1) of the APSEM). Hence, respecting the integrity of the stored data is a prerequisite for avoiding legal liability. Under Article 13(2) of the APSEM, "no liability for stored data shall be assigned to those who, subject to the conditions referred to in paragraph 1, immediately remove, or prevent access to, such data, on becoming aware that the data have been removed from the original source of transmission, or access to them has been prevented, or when a court or other competent authority ordered that such data be removed, or access to them be prevented".

Article 14 of Directive 2000/31/EC should be interpreted as implying that the rule laid down by it applies to the provider of an Internet referencing service if such a provider supplies such services without playing an active role, which could provide them with knowledge about or control over the information stored. If a service provider does not play such a role, it may not be held liable for the contents of the information stored at an advertiser's request unless immediate measures were not taken to remove or prevent access to such information once the service provider became aware of the illegal nature of such information or the advertiser's business.

Thus, the scope of liability of website providers is influenced by the type of their services. This also applies to various fields of content regulation. Assuming we are dealing with a website which meets all the definitional requirements of the press, the activities of such a provider are subject to press registration under the procedure set out in the Press Law Act (Article 20 of the Press Law Act – the regional court register; providers of audiovisual media services are exempt from this obligation under Article 24 of the Press Law Act, consolidated text, Journal of Laws of 2018, item 1914). In this case, liability rests with

the publisher and the editor-in-chief. As regards audiovisual media services, the applicable regulation is set out in the Broadcasting Act (consolidated text, Journal of Laws of 2022, item 1722); Article 41 of the BA – KRRiT (National Broadcasting Council) register or licence, depending on the type of dissemination – the register for programmes disseminated only on communication and information systems; licences for dissemination on communication and information systems and the broadcasting of programmes on operator systems) (Article 33 of the BA – KRRiT licence). Broadcasting liability will also apply here, and each case will involve editorial responsibility. It is slightly different with liability for making on-demand audiovisual content available. While business restrictions do not apply here, the rules of liability do because of extending the BA rules to providers of on-demand audiovisual media services. Under Directive 2010/13/EU, the extension of regulations to non-linear media services was meant to be restricted to on-demand audiovisual media services, excluding on-demand audio media services.

The extension included:

1) a stipulation that on-demand audiovisual media services also serve the functions assigned to broadly-defined radio and television broadcasting and, as such, they constitute parts thereof;
2) consistently replacing the word *programme* with the phrase *media service* (or, optionally, adding on-demand audiovisual media services next to programmes), and the word *broadcaster* with the phrase *media service provider*. Where the regulation applies to both programmes and on-demand audiovisual media services, or providers of both types of service, this extends to:
   a) freedom of reception (Article 1(2) of the BA),
   b) jurisdiction (Article 1a of the BA),
   c) the powers of the National Broadcasting Council (KRRiT) (Articles 6 and 10(2–4)of the BA),
   d) legal liability (Article 53(1) and Article 53a of the BA);
3) providing a reference to the appropriate application of some of the basic programme-related requirements to on-demand audiovisual media services in respect of the protection of minors and the promotion of European broadcasts: the freedom of the broadcaster to shape the on-demand media service (Article 47a and 47b of the BA); the identification obligations of the on-demand media service provider (Article 47c of the BA); the obligation of the easy recognisability of commercial communications (Article 47k of the BA); the general rules applicable to commercial communications: advertisements, sponsoring, telesales, product placement (Article 47k of the BA); the prohibition of discrimination and incitement to hate (Article 47h of the BA); the obligation to ensure that the services are available to people with visual and hearing disabilities (Article 47g of the BA); requiring that on-demand media service providers follow the rule of editorial business, within the meaning of the Press Law Act (Article 47a of the BA); the obligation to record broadcasts and

advertisements (Article 47i of the BA); and the obligation to issue reports to KRRiT (Article 47j of the BA).

Concerning on-demand services, Directive 2010/13/EU already provides for the same high level of protection for many elements, including service provider identification, the total prohibition of incitement to hatred, and quality standards applicable to audiovisual commercial communication. Notably, under Article 3(1) of the APSEM, the provisions of this Act do not apply to the dissemination or distribution of radio or television programmes, or any related text communications. However, this regulation relates exclusively to traditional radio and television communications, which are not provided on demand. Conversely, new media services, which fall under the Broadcasting Act following the implementation of Directive 2010/13/EU, fulfil the requirements of the Act on the Provision of Services by Electronic Means, and should be governed by them, including by provisions on the limitation of liability.

Another piece of EU legislation governing liability for online content-sharing is Directive 2001/29/EC, which introduces limitations on liability for copyright infringement. Article 5(5) of Directive 2001/29/EC allows the exemptions related to illegal use, provided for in Article 5(1–4), including the exemption for making copies for private use, as referred to in Article 5(2b) of this Directive, subject to the following three conditions: 1) such an exemption may be applied in certain exceptional cases only; 2) it does not conflict with a normal exploitation of the work; and 3) it does not unreasonably prejudice the legitimate interests of the rightsholder. As explained by Recital 44 of Directive 2001/29/EC, these three conditions correspond to the international obligations of Member States and the Union, and more specifically to the conditions applicable to all limitations of copyrights set out in Article 9(2) of the Berne Convention, more broadly known as the "three-step test," as reiterated in Article 13 of the TRIPS (the Agreement on Trade-Related Aspects of Intellectual Property Rights www.eur-lex.europa.eu) and in Article 10 of the WCT (the WIPO Copyright Treaty, Geneva 91996, www.eur-lex.europa.eu). The test will also apply to situations involving the use of digital content.

The examples provided above support the claim that, in each case, the same entity will be subject to different liability, depending on whether it is engaged in the service activities referred to in the APSEM, is a broadcaster or publisher, provides on-demand media services, or only provides a file-sharing platform. As a result of technological and economic convergence, the same entity can serve several different functions. Thus, its status – and, by extension, the scope of liability – is not definite. This calls for appropriate regulations providing that synchronisation is ensured at each stage of substantive legislative work. This is critical to establishing a cohesive regulatory framework which facilitates the development of the digital media sector while having due regard to the elementary principles of liability for disseminating digital content, in particular in the social media environment.

4 The rights of service users in the digital environment

Digital service users no longer play a passive role in the content communication process. Instead, they have become actively involved as both the sources and recipients of content in the digital ecosystem. Indeed, information society services base the entire design, business model, and optimisation of their services around the dual role of their users.

Regarding copyright protection, Internet users' activities have directly impacted the regulatory exemptions related to the digital non-commercial and proportionate use of quotations and extracts from copyright-protected works or other subject-matter by individual users. Under the Copyright Directive, subject to Article 13, Member States may provide an exception for content uploaded by users where such content is used for criticism, review, illustration, caricature, parody, or pastiche. Here, the question arises about the limits of such acceptable criticism, thus far primarily the domain of online journalistic activities. This change in the perception of Internet users' rights implies a shift in the roles played by various players in the existing digital environment and digital media.

It seems that attributing regulations directly to the need for a comprehensive remedy to issues around social media, and considering the lack thereof at the EU level as a legitimate reason for national regulations' going beyond implementing the Directive, is something of a simplification. Rather, definite guidelines should be followed on the scope of regulations, not necessarily involving comprehensive regulatory solutions anchored in national laws. Of course, it does not mean that this approach is wrong. However, it is more reasonable to rely on the regulatory minimum, given the need for arrangements regarding the use of digital content on European platforms. Recently, it has become necessary in this regulatory field to broaden the notion of a market for various types of content since its scope goes beyond the existing notion of a digital content market. This has been proposed in the draft Regulation of the European Parliament and of the Council on cross-border portability of online content services in the internal market (OJ L 168, 30/6/2017, pp. 1–11).

The document concerns the cross-border portability of online content services to which consumers have lawful access or content that they have purchased or rented online in their country of residence, and content they wish to continue to have access to when travelling within the EU. It also claims that the absence of or problems with the cross-border portability of online content services in the EU result from the licensing practices of copyright or related rightsholders and/or the commercial practices of service providers. Such services include websites which use works or other protected subject-matter only in an ancillary manner, such as graphical elements or music used as background, where the main purpose of such websites is, for example, the sale of goods. This means that practically every other use would be subject to the Digital Single Market regulations applicable to digital content, falling under framework regulation under this Directive.

The dichotomy of online services is recognised by the "Digital Single Market Strategy for Europe" (COM/2015/0192 final), which is built on three regulatory pillars: (1) providing better access to digital goods and services across Europe; 2) creating the right conditions and a high-level playing field for digital networks and innovative services to flourish; and 3) maximising the growth potential of the digital economy. It should be noted that the Union regulation concerns the regulation of the Digital Single Market, whilst the regulation of content (e.g., content protected by copyrights and related rights, and not only) should be considered as a matter of national-level solutions, having due regard to the specific needs of a given state, including in particular its national culture and cultural security.

An important factor in the context of users sharing their digital content online is the rule under which copyright-protected content is subject to licensing. In accordance with the Directive on Copyright in the Digital Single Market, the use of protected content by information society services providing automated image referencing is subject to obtaining a licence from rightsholders. Member States shall ensure that the information society service providers that automatically reproduce or refer to significant amounts of copyright-protected visual works, and make them available to the public for indexing and referencing purposes, conclude fair and balanced licensing agreements with any requesting rightsholders to ensure their fair remuneration. Such remuneration may be managed by the collective management organisation of the rightsholders involved, considerably facilitating the use of such content on online platforms.

Consideration should be given to issues concerning individual licences issued by competent, i.e., central authorities (followed by extended collective licences). The former determines state influence on how the digital content market functions but does not directly involve performing specific public tasks. While it seems debatable whether both legal solutions have the same strengths and weaknesses, they have the undeniable asset of affording users and owners of works considerable legal certainty, ensured by a single state authority which issues licences to use works on the Digital Single Market.

Another factor affecting the legal situation of Internet users is the processing of their personal data. A critical element in regulating Internet users' online activities is protecting their data. Under the GDPR (OJ L 119, 4.5.2016, pp. 1–88), data provided by data subjects are subject to specific rules. In particular, these include the right to data portability, which is limited to data "provided" by the data subject (rightsholder) to the data controller. In other words, it seems that user-provided data are the only information explicitly recognised as a "commodity", a kind of digital good owned by individuals.

On the one hand, this is the only dataset "portable" from one platform to another. On the other, it is the only type of (personal) data falling under a regulation which legitimises exchange, other than monetary, for supplying such digital content. Of course, "user-

generated" content does not always constitute personal data (as defined by Article 4 of the GDPR), just like not all user-provided personal data are valuable regarding intellectual property. Thus, a whole new field is opened for investigating content which is marketed in the digital economy but does not meet the definitional requirements set out by the regulations, currently accounting for various aspects of content sharing. This is particularly the case when user-provided private content is exchanged as a digital currency between data subjects (or users) and data controllers.

What should be stressed here is the importance of anonymity in processing personal data for commercial purposes. On the one hand, it is fundamental to support automated settings disabling personal data collection in the context of using online platform interfaces. On the other, such anonymity makes it harder to track Internet users who make illegal content available. This triggers a question of whether such protection creates a liability to pass entirely to digital service providers or whether the user bears some liability, too. "You don't have to share all data. But if you do, and data is sensitive, you should be able to do so in a manner where data can be trusted and protected. We want to give businesses and citizens the tools to stay in control of data. And to build trust that data is handled in line with European values and fundamental rights", said Margrethe Vestager, Executive Vice-President for A Europe Fit for the Digital Age. Her stance was supported by Commissioner for Internal Market Thierry Breton, "We are defining today a truly European approach to data sharing. Our new regulation will enable trust and facilitate the flow of data across sectors and Member States (...). With the ever-growing role of industrial data in our economy, Europe needs an open yet sovereign Single Market for data. (...) our regulation will help Europe become the world's number one data continent". The new Regulation will create the basis for a new European mode of data governance, in line with EU values and principles, such as personal data protection, consumer protection, and competition rules. This new approach proposes a model based on the neutrality and transparency of data intermediaries, which, as organisers of data sharing or pooling, may not deal in data on their own account (e.g., by selling them to another company or using them to develop their own products based on such data). Other legal solutions envisaged in the draft Regulation include measures to facilitate the reuse of certain data held by the public sector and voluntarily making data owned by natural persons and businesses available for the wider common good ("data altruism"). Building uniform European data spaces has become one of the essential components of the EU project aimed at facilitating data exchange between businesses and the private and public sectors.

The new regulations contained in Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information (OJ EU of 2019 L 172, p. 56, hereinafter: the Reuse Directive) and the Data Governance Act (COM/2020/767 final), significantly change the rules on the digital content-sharing market. The latter piece of legislation aims to establish a framework encouraging the enhanced reuse of data by increasing trust in data intermediaries, and by strengthening

data sharing mechanisms across the EU. The law will play a key role in enabling and guiding the creation of EU-wide common interoperative data spaces in strategic sectors, including those using Artificial Intelligence (AI).

The proposal lays down the rules applicable to the conditions for the reuse of protected public-sector data, including in relation to commercially confidential data, intellectual property, and data protection, as well as the obligations of data sharing providers, defined as entities providing various types of intermediary services. It also introduces the concept of data altruism and the possibility of registering an organisation as a "Data Altruism Organisation", recognised in the EU. Another proposal was to establish the European Data Innovation Board, a new formal group of experts headed by the European Commission. It is worth noting that "data" are defined in the draft as "any digital representation of acts, facts, or information, and any compilation of such acts, facts, or information, including in the form of sound, visual, or audiovisual recording". It is a broad definition which includes personal data as set out in the GDPR. Therefore, the GDPR and the Act can apply simultaneously. The explanatory memorandum also states that "measures are designed in a way that fully complies with data protection legislation and strengthens in practice the control natural persons have over the data they generate".

5 Notice and takedown in the business of online content-sharing service providers

The issue of sharing digital content online concerns primarily the relationships between online content-sharing service providers and data subjects with regard to intellectual property, as outlined in the Directive on Copyright in the Digital Single Market. It can be assumed that the foremost responsibility of rightsholders is to provide online content-sharing providers with the information they need to identify content. Providers, in turn, should ensure transparency for the implemented identification and follow-up measures. When assessing the proportionality and effectiveness of the implemented measures, technological constraints and other difficulties should be taken into account, as should the number and type of works or other protected subject-matter shared by content users. Under Article 15 of Directive 2000/31/EC, the implementation of measures by service providers should not consist of a general monitoring obligation but should be limited to ensuring the non-availability of unauthorised uses of their services of specific and duly notified copyright-protected works or other subject-matter.

Thus, it is fundamental to maintain the balance between users' rights and rightsholders' rights to content under the Charter of Fundamental Rights of the European Union (www.eur-lex.europa.eu).

Notably, the implemented measures should not require the identification of individual users sharing content online and should not involve the processing of data about individual users under the GDPR and Directive 2002/58/EC. In particular, where a given

content is subject to sharing restrictions, online content-sharing service providers should be required to provide a complaint mechanism intended for users whose data integrity has been compromised. Such a mechanism should allow users to determine why certain content is targeted by these measures and make it easier to find basic information about notable exceptions and applicable limitations.

If authors or performers issue a licence or transfer rights, they expect their work or performance to be exploited. It happens, however, that works or performances which have been licensed or transferred are not exploited at all. And when these rights have been transferred on an exclusive basis, authors and performers cannot turn to another partner to exploit their work. In such a case, and after a reasonable period of time has elapsed, authors and performers should have the right of revocation. Revocation should also be possible when the transferee or licensee has not complied with their reporting or transparency obligation, as provided for in Article 14 of the Directive on Copyright in the Digital Single Market. Revocation should only be considered after all the steps of alternative dispute resolution have been completed, particularly concerning reporting. As exploitation of works can vary depending on the sectors, specific provisions could be taken at the national level to reflect the specificities of the sectors, such as the audiovisual sector, or the works and the anticipated exploitation periods, notably providing for time limits for the right of revocation. Online content-sharing service providers perform an act of communication to the public, or an act of making content available to the public, for the purposes of this Directive, when they give the public access to copyright-protected works or other protected subject-matter uploaded by users. Hence, liability arising from dissemination will also apply to content which remains outside the control of, and is not moderated by, the provider. Therefore, an online content-sharing service provider must obtain authorisation from the rightsholders, for instance, by concluding a licensing agreement, to disseminate works or other protected subject-matter or to make them available to the public. When authorisation is obtained by way of a licensing agreement, that authorisation also covers acts carried out by users of the services falling within the scope of Article 3 of Directive 2001/29/EC, when they are not acting on a commercial basis or where their activity does not generate significant revenues. When an online content-sharing service provider performs an act of communication to the public or an act of making content available to the public, the limitation of liability established in Article 14(1) of Directive 2000/31/EC does not apply to situations involving copyrights. This rule, however, applies to providers of services beyond the scope of the Directive on Copyright in the Digital Single Market. If no authorisation is granted, online content-sharing service providers are liable for unauthorised acts of communication to the public, including making copyright-protected works and other subject-matter available to the public, unless the service providers demonstrate that they have a) made best efforts to obtain an authorisation, and b) made best efforts, following high industry standards of professional diligence, to ensure the unavailability of specific works and other subject-matter for which the rightsholders have provided the service providers with the relevant and necessary information, and c) in any event acted expeditiously, upon receiving a

sufficiently substantiated notice from the rightsholders, to hinder access to, or to remove from their websites, the notified works or other subject-matter, and made best efforts to prevent their future uploads.

Under Article 22 of the Directive on Copyright and Related Rights in the Digital Single Market, where an author or a performer has licensed or transferred their rights in a work or other protected subject-matter on an exclusive basis, the author or performer may revoke, in whole or in part, the licence or the transfer of rights where there is a lack of exploitation of that work or other protected subject-matter.

In determining whether the service provider has complied with these obligations, the following should be particularly taken into account: a) the type, audience and size of the service, and the type of works or other subject-matter uploaded by the users of the service; and b) the availability of suitable and effective means, and their cost for service providers.

For new online content-sharing service providers whose services have been available to the public in the Union for less than three years, and which have an annual turnover below EUR 10 million, calculated under Commission Recommendation 2003/361/EC (20) (OJ L 124, 20/05/2003, p. 36), the conditions under the liability regime set out in Paragraph 4 are limited to compliance with Point (a) of Paragraph 4, and to acting expeditiously, on receiving a sufficiently substantiated notice, to hinder access to the notified works or other subject-matter, or to remove those works or other subject-matter from their website.

Where the average number of monthly unique visitors of such service providers exceeds 5 million, calculated based on the previous calendar year, they shall additionally demonstrate that they have made best efforts to prevent further uploads of the notified works and other subject-matter for which the rightsholders have provided relevant and necessary information.

Due to the right to communication and freedom of expression, cooperation between online content-sharing service providers and rightsholders might not prevent works or other subject-matter uploaded by users, which do not infringe copyright and related rights, from being available. This includes such works or other subject-matter that are covered by an exception or limitation. Users in each Member State should be able to rely on any of the following existing exceptions or limitations when uploading and making available content generated by users on online content-sharing services: a) quotation, criticism, review; and b) use for caricature, parody or pastiche purposes. Online content-sharing service providers are required to provide rightsholders, at their request, with adequate information on the functioning of their practices concerning the cooperation referred to in Paragraph 4 and, where licensing agreements are concluded between service providers and rightsholders, with information on using content covered by the agreements. Furthermore, they must put in place an effective and expeditious complaint and redress mechanism available to users of their services in the event of disputes over the disabling

of access to, or the removal of, works or other subject-matter uploaded by them. Where rightsholders request to have access to their specific works or other subject-matter disabled, or to have those works or other subject-matter removed, they must duly justify the reasons for their requests. Complaints submitted under the mechanism envisaged in the first subparagraph must be processed without undue delay, and decisions to hinder access to or remove uploaded content are subject to human review. Member States also ensure that out-of-court redress mechanisms are available for settling disputes. Such mechanisms must enable disputes to be settled impartially and may not deprive users of the legal protection afforded by national law, without prejudice to the users' rights to have recourse to efficient judicial remedies. In particular, Member States must ensure that users have access to a court or another relevant judicial authority to assert the use of an exception or limitation to copyright and related rights.

Specific provisions for the revocation mechanism may be provided for in national law, taking into account the following: a) the specificities of the different sectors and the different types of works and performances and where a work or other subject-matter contains the contribution of more than one author or performer, the relative importance of the individual contributions, and the legitimate interests of all authors and performers affected by the application of the revocation mechanism by an individual author or performer. Member States may exclude works or other subject-matter from the application of the revocation mechanism if such works or other subject-matter usually contain contributions of a plurality of authors or performers. Member States may further provide that the revocation mechanism can only apply within a specific time frame, where such restriction is duly justified by the specificities of the sector or the type of work or other subject-matter concerned. Member States may provide that authors or performers can choose to terminate the contract exclusivity instead of revoking the licence or transfer of the rights.

The author or the performer must notify the person to whom the rights have been licensed or transferred and set an appropriate deadline by which the exploitation of the licensed or transferred rights is to take place. After the expiry of that deadline, the author or the performer may choose to terminate the contract exclusivity instead of revoking the licence or transfer of the rights. Member States may provide that any contractual provision derogating from the revocation mechanism is enforceable only if it is based on a collective bargaining agreement.

As noted by G. Frosio and S. Mendis, Article 17(9) of the Directive represents the legislative culmination of a global trend that inclines towards the implementation of digital content monitoring and filtering systems by intermediaries, digital content providers, meaning the transformation of the role and status of digital service providers as being liable for the content made available. Such a shift in roles in the digital market requires a fair balance between the diverse interests of users and intermediaries in disseminating and using copyright-protected content online (Frosio, Mendis, 2020:565).

Issues around the new regulations on digital content-sharing online, including the liability of digital service providers, have long been the subject of inquiry into the new field of exploitation of works. There has been a tendency in recent years to authorise digital service providers to pre-monitor all content uploaded by users. This seems to be a precondition for such content to be used appropriately. Providers could be absolved from direct and indirect copyright liability on condition that they could be shown to have implemented the appropriate content recognition and filtering technology to counter online infringements of copyrights. It involves "notice and staydown" responsibilities, where regular notifications of copyright subjects about removing illegal files would entail the obligation of proactively identifying and eliminating any instances of content purported to violate the law, and preventing the upload of such content in the future. It should be mentioned that the EC has officially confirmed, in its Communication on tackling illegal content online COM(2017) 555 final), that providers should "voluntarily" fulfil these obligations and that their scope should not be limited to copyright issues but should also include identifying and removing illegal material, such as terrorist and hate speech material. Online platforms may become aware of illegal content in several different ways, through different channels. Such channels for notifications include (i) court orders or administrative decisions; (ii) notices from competent authorities (e.g., law enforcement bodies), specialised "trusted flaggers", intellectual property rightsholders or ordinary users; and (iii) the platforms' investigations or knowledge.

Similar measures were applied under provider self-regulation schemes. An example is Google rules, under which rightsholders should upload content by sharing reference files with metadata in order to use Content ID. Google explained that even small elements of content use could be detected, regardless of whether or not any significant modifications had been made. Under YouTube's business model, rightsholders may prevent the display of copyright-protected materials on YouTube to control how their content is used, without being able to take any other measures or to make a profit from advertisements accompanying their content. New content uploaded to YouTube is checked on a fingerprint database, and then YouTube implements business rules to protect rightsholders. This video-sharing platform also has a policy in place for notifying illegal content. YouTube has several Policies on digital content sharing on its platform.

"You might not like everything you see on YouTube. If you think content is inappropriate, use the flagging feature to submit it for review by our YouTube staff. Our staff carefully reviews flagged content 24 hours a day, 7 days a week, to determine whether there's a violation of our Community Guidelines. Our products are platforms for free expression. But we don't support content that promotes or condones violence against individuals or groups based on race or ethnic origin, religion, disability, gender, age, nationality, veteran status, caste, sexual orientation, or gender identity, or content that incites hatred based on these core characteristics. It's not okay to post violent or gory content that's primarily intended to be shocking, sensational, or gratuitous. If posting graphic content in a news

or documentary context, please be mindful to provide enough information to help people understand what's going on in the video. Don't encourage others to commit specific acts of violence. YouTube is not for pornography or sexually explicit content. If this describes your video, even if it's a video of yourself, don't post it on YouTube. Also, be advised that we work closely with law enforcement, and we report child exploitation. Don't post videos that encourage others to do things that might cause them to get badly hurt, especially kids. Videos showing such harmful or dangerous acts may get age-restricted or removed depending on their severity. Everyone hates spam. Don't create misleading descriptions, tags, titles, or thumbnails to increase views. It's not okay to post large amounts of untargeted, unwanted or repetitive content, including comments and private messages. It's not ok to post abusive videos and comments on YouTube. If harassment crosses the line into a malicious attack, it can be reported and may be removed. In other cases, users may be mildly annoying or petty and should be ignored. Respect copyright. Only upload videos that you made or that you're authorised to use. This means abstaining from uploading videos you didn't make or using content in your videos that someone else owns the copyright to, such as music tracks, snippets of copyrighted programs, or videos made by other users, without necessary authorisations.

Things like predatory behaviour, stalking, threats, harassment, intimidation, invading privacy, revealing other people's personal information, and inciting others to commit violent acts or to violate the Terms of Use, are taken very seriously. Anyone caught doing these things may be permanently banned from YouTube.

If someone has posted your personal information or uploaded a video of you without your consent, you can request removal of content based on our Privacy Guidelines. Accounts that are established to impersonate another channel or individual may be removed under our impersonation policy. Learn about how we protect minors in the YouTube ecosystem. Also, be advised that we work closely with law enforcement, and we report child endangerment".

As suggested by these documents, on the one hand, the platform presents itself explicitly as an intermediary. On the other, in addition to self-regulation, the issues mentioned above are, to some extent, addressed by the Audiovisual Media Services Directive (OJ L 95, 15/4/2010, pp. 1–24), laying down the rules of liability for video sharing platform operators.

The binding rules for protecting intellectual property online are diverse and highly fragmented. For example, Google has reached an agreement with the French audiovisual industry to provide rightsholders with direct access to content removal and blocking tools on YouTube. Yet, the list of the most popular torrent sites, compiled to track the popularity of these websites, is still long. Some of them contain links to adware. As of early 2020, the most popular torrent sites were The Pirate Bay, YTS.lt (dedicated to globally popular film productions; YTS has been recently litigated against in three cases

in the US), 1337x, RARBG (the site operates from several popular domains, but only the one with the highest traffic is listed); Torrentz2, EZTV.io, LimeTorrents, Fitgirl, and Tamilskie Rockers.

As regards the assessment of copyright protection solutions for digital content, the implementation of the procedures provided for in the Directive on Copyright in the Digital Single Market would be compatible with the right of online platforms, including in particular social networking sites, to establish the framework of liability, and with the right of Internet users to fair trial, privacy, and freedom of expression under Articles 6, 8 and 10 of the 1950 European Convention on Human Rights (ECHR) (Polish Journal of Laws of 1993, No. 61, item 284), i.e., the right to a fair trial, respect for private and family life, and freedom of expression.

The key question is whether suspension and refusal-of-access procedures for digital content are compatible, in particular with the right to hold opinions, and to receive and impart information and ideas without interference by public authorities, regardless of frontiers. The lawfulness of implementing a notice and staydown regime would largely depend on whether the technology in question conforms with the three-step test performed by the ECHR in Strasbourg. In accordance with the ECHR, any interference with Articles 8 and 10 must be "in accordance with the law", serve one or more of the legitimate interests referred to in Article 8(2) and Article 10(2), and be both "necessary" and "proportionate". The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

6 Issues around notice and takedown, and the right to privacy, freedom of speech, and ownership rights

In 1788, James Madison, a co-author of the US Constitution, wrote, "If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed, and in the next place oblige it to control itself". And this thought remains as relevant as ever concerning future social media regulations.

It should be noted that the adoption of digital content recognition and filtering technology, by its very nature, raises serious concerns about not only the right to privacy but also the right to freedom of expression. First, content notice and staying down might lead to issues with the right to privacy. This concerns, for instance, social media users who illegally

upload copyrighted content through a social networking platform and disable access to such content (www.internetsociety.org/about-internet-society/annual-review/2010). This stems from the fact that content recognition and filtering generally rely on fingerprinting technology, watermarks, real-time monitoring, and identifying illegal user content before blocking access. In particular, unlike blocking measures, DPI (deep packet inspection) systems are a type of data processing that inspects in detail the data being sent over a computer network and can take actions such as alerting, blocking, re-routing, or logging it accordingly. Deep packet inspection is often used to baseline application behaviour, analyse network usage, troubleshoot network performance, ensure that data are in the correct format, check for malicious code, eavesdropping, and Internet censorship (Duncan Geere, https://www.wired.co.uk/article/how-deep-packet-inspection-works), and investigate network packets instead of focusing on the source, such as a URL blacklist. The DPI technology can reveal information which makes it easy to establish user identity, location, interests, activities, etc. The general obligation to retain data is, however, incompatible with the personal data protection system unless it fulfils specific conditions. See an opinion of Advocate General Henrik SaugmandsgaardØe, delivered on 19 July 2016: "Mr Schrems, an Austrian national residing in Austria, is a user of the social network Facebook. All users of that social network residing in the territory of the European Union are required, when signing up, to enter into a contract with Facebook Ireland, a subsidiary of Facebook Inc., which is established in the United States. Those users' personal data are transferred, in whole or in part, to servers belonging to Facebook Inc., situated in the territory of the United States, where they are processed. On 25 June 2013, Mr Schrems filed a complaint with the DPC whereby he requested her, in essence, to prohibit Facebook Ireland from transferring the personal data relating to him to the United States. He claimed that the law and practices in force in the United States did not ensure adequate protection of the personal data retained in its territory against intrusions resulting from the surveillance activities practised by the public authorities. Mr Schrems referred in that regard to the revelations made by Mr Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency (NSA)" (Case C-311/18).

In that regard, the Court held, in the judgment in Schrems (see: C-203/15 and C-698/15 Tele2 Sverige AB v. Post-ochtelestyrelsen (C-203/15) and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15), with the participation of Open Rights Group, Privacy International, Law Society of England and Wales) that the legislation which does not provide for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him (Article 15 of the GDPR, entitled "Right of access by the data subject," stipulates in Paragraph 1 that "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data [...]". The "access principle" provided for in Annex II (II) (a) of the Privacy Shield has the same underlying purpose) or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right

enshrined in Article 47 of the Charter. It must be emphasised that that right of access entails the possibility for a person to obtain from the public authorities, subject to the derogations that are strictly necessary to pursue a legitimate interest, a confirmation of whether they are or are not processing data of a personal nature relating to him or her. And it does not matter here whether the person concerned is unaware of whether the public authorities have retained personal data relating to him or her, following, inter alia, an automated filtering process of electronic communications flows.

What's more, notably, J. Urban, J. Karaganis, and B. Schofield claim that notice and takedown also raise concerns as to freedom of expression, since user choices are made by algorithm matching based on big data, and not only in a context understandable exclusively to humans (Urban, Karaganis, Schofield, 2016:8). What is interesting is that each week Google receives millions of take-down requests, sent mainly by or on behalf of major entertainment corporations (Urban, Karaganis, Schofield, 2016:11). Thus, the use of this technology might easily lead to mistakes, especially to blocking legal content (falsely positive), or sharing illegal materials (falsely negative). It is emphasised that the right to freedom of expression might be infringed when exemptions apply which are not protected under copyright laws or laws on personal data protection, e.g., when content belongs to a public domain or is misdetected and removed, leading to "false results", as mentioned above. What is also important is that some systems are highly efficient in recognising content but targeting illegal remixes, DJ sets, and mashups can still be very difficult in the case of copyright-protected content and other content which features hate speech that is not explicit but contextual.

The ECHR also noted these circumstances in the case Delfi v. Estonia, where the Court held that "Delfi's news portal had a disclaimer stating that the writers of the comments – and not the applicant company – were accountable for them and that the posting of comments that were contrary to good practice or contained threats, insults, obscene expressions or vulgarities, or incited hostility, violence or illegal activities, was prohibited. Furthermore, the portal had an automatic system of deletion of comments based on stems of certain vulgar words, and it had a notice-and-take-down system in place, whereby anyone could notify it of an inappropriate comment by simply clicking on a button designated for that purpose to bring it to the attention of the portal administrators. On some occasions, the administrators removed inappropriate comments on their own initiative. Thus, the applicant company could not be said to have wholly neglected its duty to avoid causing harm to third parties. Nevertheless, and more importantly, the automatic word-based filter used by the applicant company failed to filter out odious hate speech and speech inciting violence posted by readers, and thus limited its ability to expeditiously remove the offending comments. Notably, the majority of the words and expressions in question did not include sophisticated metaphors or contain hidden meanings or subtle threats. They were manifest expressions of hatred and blatant threats to the physical integrity of the injured party. Thus, even if the automatic word-based filter may have been useful in some instances, the facts of the present case

demonstrate that it was insufficient for detecting comments whose content did not constitute protected speech under Article 10 of the Convention". Google similarly claimed that imposing the obligation to notify and block service providers' content was illegitimate. Some mechanisms, also concerning discretion in their use, can be used in one context, such as Content ID or YouTube, but not in another, e.g., social networking platforms (Facebook, Twitter, Snapchat, Instagram, etc.). Google explains that it is still easier than ever for authors to connect with their audiences, build fanbases, and share their content online using these networking platforms (EC 2016b, 164–165).

The DSA states, "Union citizens and others are exposed to ever-increasing risks and harms online. According to the EU legislators, the Digital Services Act introduces important safeguards to allow citizens to freely express themselves while enhancing user agency in the online environment, as well as the exercise of other fundamental rights such as the right to an effective remedy, non-discrimination, rights of the child as well as the protection of personal data and privacy online. The proposed Regulation will mitigate risks of erroneous or unjustified blocking of speech, address the chilling effects on speech, and stimulate the freedom to receive information and hold opinions. The proposal will only require the removal of illegal content and will impose mandatory safeguards when users' information is removed, including the provision of explanatory information to the user, complaint mechanisms supported by the service providers, as well as external out-of-court dispute resolution mechanisms. Furthermore, it will ensure EU citizens are also protected when using services provided by providers not established in the Union but active on the internal market since those providers are covered too. Obviously, this applies, above all, to major social networking platforms. Therefore, an important objective of the DSA was to introduce uniform notice and action (notice and takedown) mechanisms across the EU" (COM(2020) 825 final).

Hence, it is imperative to provide clear and user-friendly mechanisms for users to notify or flag illegal content to intermediaries. Online intermediaries have been obliged to verify the notified content, and to respond to the notifying party and content provider within a reasonable time, explaining why the notified content had to be blocked or removed or why it remained online. It is critically important to put procedures in place for intermediaries to appeal against moderation decisions. What is important is that the steps taken by online content-sharing service providers, cooperating with rightsholders, should be without prejudice to the application of exceptions or limitations to copyright, particularly those which guarantee the freedom of user expression. Users should be allowed to upload and make available the content generated by users for the specific purposes of quotation, criticism, review, caricature, parody or pastiche. That is particularly important for striking a balance between the fundamental rights laid down in the Charter of Fundamental Rights of the European Union, in particular the freedom of expression and the freedom of the arts, and the right to property, including intellectual property. In judgments in the cases Sabam v. Netlog and Sabam v. Scarlet, the CJEU

refused to impose on those service providers the obligation to automatically monitor the content disseminated by their users under Articles 8, 11, and 16 of the Charter.

Digital content moderation alone is problematic from a regulatory standpoint. Indeed, as noted by N. Elkin-Koren and M. Perel, it blurs the distinction between private interests and public responsibilities, delegates the power to make social choices about content legitimacy to obscure algorithms, and circumvents the constitutional safeguard of the separation of powers (Elkin-Koren, Perel, 2020:671). A prime example of this was seen when Facebook and Twitter blocked the accounts of the then-incumbent US President Donald Trump or when they took down historical content about children's concentration camps in Łódź for political reasons. Another instance involved the blocking of a short animation produced by the Polish Institute of National Remembrance (IPN) concerning Poland's modern history ("Niezwyciężeni" – "The Unconquered"), which premiered on 15 September 2010. Commissioned by IPN, the video was made in two languages, Polish and English. YouTube recently blocked the latter due to "a copyright claim". "The Unconquered" is about Poland's history from World War II to the fall of the Iron Curtain. Its Polish version on YouTube was viewed almost 1.2 million times (and received 68,000 likes and 1,000 dislikes). The animation video became popular immediately after its première, not only among Polish users. On IPN's profile alone, it had nearly 35,000 views. It took one click to remove a video having more than 2 million views on Facebook from IPN's YouTube account. M. Poślad, Head of CEE & Transatlantic Public Policy at Google, wrote that the platform was legally obliged to take down the material.

Marta Poślad
@MartaPoslad
YouTube is required by law to block notified videos. Awaiting the IPN's response to the copyright claim https://goo.gl/jQEEYa

niezależna

Niezalezna.PL
@niezaleznapl
YouTube blocks video on Poles' heroism. The Internet is on fire http://fb.me/BYmhTAs2
4:26 PM · 23 Sept. 2017

It should be emphasised that, in the case Sabam v. Netlog (OJ C 98, 31.3.2012, pp. 6–7), the CJEU examined whether or not requiring a social networking platform which shared third-party content to use notice and takedown measures to enforce copyrights online represented an infringement of fundamental rights. The CJEU concluded that the identification, systematic analysis, and processing of personal information connected with the profiles of Netlog users could represent an infringement of their right to privacy in the context of Article 8 of the Charter of Fundamental Rights. This judgment also reiterates CJEU's previous decision in the case Sabam v. Scarlett (Case C-70/10), and later it was reiterated in CJEU's ruling in the Mc Fadden case (Case C-484/14). Moreover, the objectives which, under that provision, such measures must pursue, such as safeguarding national security, defence, and public security, and the prevention, investigation, detection and prosecution of criminal offences or unauthorised use of the electronic communications system, overlap substantially with the objectives which legitimise restrictions on the rights and freedoms set out in Article 31(3) of the Constitution of the Republic of Poland. On the one hand, the retention of communications data enables the government to control the governed by providing the competent authorities with a means of investigation which might prove useful in fighting serious crime, particularly in combating terrorism. In substance, the retention of communications data gives the authorities a certain ability to examine the past by accessing data relating to user communications. However, on the other hand, it is imperative to oblige the government to control itself with respect to both the retention of data and access to the data retained, given the grave risks engendered by the existing databases encompassing all communications made within the national territory. Indeed, these enormous databases give anyone with access the power to instantly catalogue every member of the population in question. These risks must be scrupulously addressed, in particular through examining the strict necessity and proportionality of the general obligation for digital content providers to block and remove content, and to provide data to public authorities.

Accordingly, it is necessary to strike a fair balance between the obligation of Member States to ensure the protection of individuals on their territory, the observance of the fundamental rights to private life and personal data protection, and the protection of intellectual property. According to ECHR's case law, for any interference with the right to privacy or freedom of expression to be "lawful" under Articles 8 and 10 of the Convention, the following three conditions must be satisfied. First, it must be based on domestic legislation; second, such legislation should be accessible; and third, the legislation should follow the Strasbourg Court's rules of predictability and legality. The adoption of notice and action systems could be incompatible with the Court's requirements regarding accessibility, predictability, and legality, thereby violating the first part of its non-cumulative test under Articles 8(2) and 10(2) of the Convention. As regards the first rule, following ECHR's case law, the quality of a legal requirement, under Articles 8 and 10 of the Convention, requires that a law be published and, by extension, that fair access to it be provided to those affected by the law. As noted above,

the assessment of the consequences concluded that, in the case at hand concerning copyright protection, rightsholders must supply service providers with the information necessary for content identification, and these services must furnish rightsholders with the "appropriate information" about systems.

What is concerning, however, is that users are refused access to the technical details of these evidence collection techniques, as a result of which they may not rely on the judicial review to question their use. In the case Sabam v. Scarlet, the Court observed that notice and takedown involved filtering all electronic communication passing through the ISP to identify individuals engaged in copyright infringement, as well as blocking all incoming and outgoing communication involving such an infringement. The reference for a preliminary ruling concerned the dispute between the company Scarlet and Sabam, a Belgian society of authors, composers, and publishers. It concerned Scarlet's refusal to install a system for filtering electronic communications which use peer-to-peer software to prevent file sharing, which infringes copyright. The national court asked the question of whether EU regulations permit national courts to be authorised to issue an injunction against intermediaries, for all its customers, *in abstracto*, and as a preventive measure, exclusively at the cost of that intermediary and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, to identify on its network the movement of electronic files containing works in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files. The Court held that such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its business. Furthermore, it would not respect the requirement that a fair balance be struck between protecting intellectual property rights and protecting the freedom to conduct business enjoyed by operators such as ISPs. Lastly, Scarlet claimed that installing a filtering system would be in breach of the provisions of the European Union law on the protection of personal data and communications secrecy, since such filtering involves the processing of IP addresses, which are personal data. In that context, the referring court regarded that, before ascertaining whether a mechanism for filtering and blocking peer-to-peer files existed and could be effective, it had to be satisfied that the obligations liable to be imposed on Scarlet were in accordance with the European Union law. Accordingly, such an injunction would result in a grave infringement of the freedom of the ISP concerned to conduct its business since it would require that ISP to install a complicated, costly and permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, requiring that measures to ensure the respect of intellectual property rights should not be unnecessarily complicated or costly.

As mentioned before, the assessment of consequences concluded that rightsholders claimed that the functioning of such technologies remains largely "unclear" to them (EC 2016a, 141). As regards the predictability rule, in accordance with ECHR case law, there must be a sufficient degree of predictability in law as to the scope of the applicable measures, as guaranteed by Articles 8 and 10 of the Convention. Worryingly, this

suggests that the level of control required to implement this technology constitutes an intrusive analysis of both personal and sensitive data. Hence, since notice, staydown, and takedown depend on the monitoring equipment, the level of investigation required to monitor users must be clearly defined. Another pertinent issue is whether installing content recognition and filtering would pass the third part of the ECHR's three-step test. According to ECHR case law, under Articles 8(2) and 10(2) of the Convention, supervisory and technical measures are "necessary" in a democratic society if they address "an urgent social need" and are proportionate means of achieving a legitimate aim. Furthermore, the ECHR noted that the state's explanation of such measures must be "adequate and relevant" although state authorities have a certain margin of discretion.

In reality, this goes along the lines of the judgment in the Delfi v. Estonia case, in which the ECHR held that, if accompanied by effective procedures allowing for rapid response, the notice and takedown would represent an appropriate tool for balancing the rights and interests of all those involved. In its judgment on the case Sabam v. Netlog, the CJEU explained that the notice and staydown solution constituted a breach of EU law since it required social networking platforms to implement filtering technology for all communications. Moreover, technology cannot handle complex decisions such as determining whether a certain use is lawful, identifying copyright ownership, and avoiding mistakes, duplicates, or overblocking (Urban, Karaganis, Schofield, 2016:35). In its judgment in the case Sabam v. Netlog, the CJEU noted that Article 15(1) of the Electronic Commerce Directive prohibits national judges from imposing general monitoring obligations on social networking platforms. According to the CJEU, because these platforms were required to implement a complex, expensive, and permanent system, their freedom to conduct business was affected significantly. In particular, it found that such technology violated Article 3(1) of Directive 2004/48/EC (OJ L 157, 30/04/2004, pp. 45–86). Filtering also involved the detection, automated analysis, and processing of personal data, likely blocking legal communications. Relying on the case Promusicae v.Telefonica (Case C-275/06), the CJEU concluded that notice and staydown did not result in a fair balance between the rightsholders right to intellectual property, on the one hand, and the freedom to conduct business by other social networking platforms, as well as the users' rights to personal data protection and to receive and impart information, on the other.

Regarding the obligations imposed on intermediaries, it is vital to recall the ECHR's decision in the case (40397/12) Neij &SundeKolmisoppi v. Sweden. During 2005 and 2006, Fredrik Neij and Peter SundeKolmisoppi were involved in running one of the world's largest file-sharing (music, movies, computer games) services on the Internet – *The Pirate Bay* (TPB). In 2008, they and others were charged with complicity in committing crimes in violation of the Copyright Act. As a result, several companies in the entertainment business brought private claims against them. In April 2009, the District Court in Stockholm sentenced them to one year's imprisonment and held them jointly liable for damages of approximately EUR 3.3 million, together with the other defendants.

In November 2010, the Court of Appeal in Svea reduced their prison sentences but increased their liability for damages to approx. EUR 5 million. In their application to the Court, both defendants argued that they were not liable for how other individuals used the TPB website, whose original purpose was to facilitate online data sharing. They claimed that crimes were being perpetrated only by those users who had exchanged illegal information about copyrighted material.

Accordingly, in reliance on Article 10 of the Convention, they argued that their conviction for complicity in committing crimes in violation of the Copyright Act represented an infringement of their right to freedom of expression (Ombelet, Kuczerawy, Valcke, 2016: 4). The Court found that Article 10 of the Convention guaranteed the right to impart information and the public's right to receive it. In light of its accessibility and capacity to store and communicate vast amounts of information, the Internet plays a significant role in enhancing public access to news and in facilitating the sharing and dissemination of information. Moreover, it applies not only to the content of the information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information. Further, Article 10 guarantees freedom of expression to "everyone". No distinction is made in it according to whether or not the aim pursued is profit-making. The Court found that the Swedish authorities were obligated to protect the plaintiffs' property rights under the Copyright Act and the Convention, and that there were weighty reasons for restricting the applicant's freedom of expression.

Moreover, the Swedish courts advanced relevant and sufficient reasons to consider that the applicant's activities within the commercially run TPB amounted to criminal conduct requiring the appropriate punishment. "In this respect, the Court reiterates that the applicants were only convicted for copyright-protected materials. In reaching this conclusion, the Court has regard to the fact that the domestic courts found that the applicants had not taken any action to remove the torrent files in question despite having been urged to do so. Instead, they had been indifferent to the fact that copyright-protected works had been the subject of file-sharing activities via TPB". Consequently, the Court also found that, due to the nature of the information contained in the shared material and the weighty reasons for the interference with the applicant's freedom of expression, this interference was "necessary in a democratic society", within the meaning of Article 10(2) of the Convention.

On the one hand, A. Lucas-Schotter claims that Article 13 of the Directive on Copyright in the Digital Single Market is a well-balanced text which, despite attracting sharp criticism, is fully compliant with Community laws and does not violate the Charter of Fundamental Rights of the European Union and the Electronic Commerce Directive (Lucas-Schoetter, 2017:21). On the other hand, there has been a growing number of disputes over content recognition and filtering systems. Ch. Angelopoulos and S. Smet opined that, using the example of copyright, the risk exists that no resolution would be

possible. "When two industries with conflicting interests are asked to self-regulate, it only entrenches the differences in their business models, and that is why "cooperation" between Internet service providers and the entertainment industry struggles to work without a court ruling" (Angelopoulos, Smet, 2016:301; Horten, 2016:142).

It is worth concluding that regulations related to the notice and action obligation, although supported by the ECHR's ruling, are criticised for completely disregarding the role of service providers and digital media in society. In the case Delfi v. Estonia, judges Sajó and Tsotsoria (Case 64569/09) observed that, in cases where an individual victim exists, they may be prevented from notifying an Internet service provider of the alleged violation of their rights. The Court attaches weight to the consideration that the ability of a potential victim of hate speech to monitor the Internet continuously is more limited than the capability of a large commercial Internet news portal to prevent or rapidly remove such comments. Therefore, a large news portal's obligation to take effective measures to limit the dissemination of hate speech and speech inciting violence – the issue in the present case – can, by no means, be equated to "private censorship". While acknowledging the "important role" played by the Internet "in enhancing public access to news, and facilitating the dissemination of information in general, it is also mindful of the risk of harm posed by content and communications on the Internet".

Another issue pertains to user anonymity. Internet users' interest in not revealing their identity seems critical. Anonymity has long been a means of avoiding reprisals or unwanted attention. As such, it can promote the free flow of ideas and information. At the same time, the ease, scope, and speed of the dissemination of information on the Internet, and the persistence of the information once disclosed, may considerably aggravate the effects of unlawful speech on the Internet compared to traditional media. Different degrees of anonymity are possible on the Internet. An Internet user may be anonymous to the broader public while being identifiable by a service provider through an account or contact data, which may be either unverified or subject to some verification – ranging from limited verification (for example, through activation of an account via an e-mail address or a social network account) to secure authentication, be it by the use of national electronic identity cards or online banking authentication data allowing somewhat more secure identification of the user. A service provider may also allow an extensive degree of anonymity for its users, in which case the users are not required to identify themselves at all, and they may only be traceable – to a limited extent – through the information retained by Internet access providers. The release of such information would usually require an injunction by the investigative or judicial authorities and would be subject to restrictive conditions. It may nevertheless be necessary in some cases to identify and prosecute perpetrators. Another aspect involves transferring personal data when illegal content has to be blocked. Under the EU-US Privacy Shield, the United States ensures a sufficient degree of protection for data the EU provides to the United States. The EU-US Privacy Shield is constituted by the principles issued by the US Department of Commerce on 7 July 2016, as set out in Annex II, and official declarations

and commitments contained in the documents presented in Annexes I, III-VII. For the purpose of Paragraph 1, personal data are transferred under the EU-US Privacy Shield, where they are transferred from the Union to organisations in the United States that are included in the "Privacy Shield List", maintained and made publicly available by the US Department of Commerce, under Sections I and III of the Principles set out in Annex II. Annex III A to this decision, entitled "EU-U.S. Privacy Shield Ombudsperson mechanism regarding signals intelligence", attached to the letter of the then Secretary of State John Kerry, dated 7 July 2016, contains a Memorandum laying down a new mediation procedure conducted before the Senior Coordinator for International Information Technology Diplomacy (Senior Coordinator), as appointed by the Secretary of State. Following the Memorandum, the procedure has been implemented "to facilitate the processing of requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCRs), 'Derogations', (2) or 'Possible Future Derogations', (3) through established avenues under applicable United States laws and policy, and the response to those requests".

It is concerning that each monitoring system which has to be implemented by social networking platforms to comply with notice and takedown obligations might be used in the future to process users' analytical data for targeted display-advertising strategies. The problem is further exacerbated by the fact that DPI technology also makes it possible to modify content. Thus, the fundamental question arises as to whether it would be relatively easy, from the technical standpoint, to apply content monitoring, recognition, and filtering technology once the underlying infrastructure has been broadly implemented in corporations or public authorities, to block access to other information, thereby silently encouraging Internet censorship (Internet Society 2010:80, www.wipo.int).

According to the ECHR, the implementation of notice and takedown systems would be in line with social networking platforms and users' right to a fair trial, and the right to privacy and freedom of expression, provided that they are informed about the technical details of such systems, as well as about the *ratione personae*, *rationemateriae* and *rationetemporis* scopes of the supervisory and technical measures, which should be set out explicitly by law. Public authorities should be involved in checking and authorising systems, followed by regular audits. Also, it should be emphasised that notice and takedown are insufficient and limited to situations in which these systems can be considered essential to achieve a legitimate aim following the necessity and proportionality principles. As a rule, it is important to implement mechanisms to prevent the overblocking of digital content. Platforms should provide their users with simple mechanisms to question decisions on removing digital content they have uploaded. However, where no agreement can be reached in this manner, cases should be referred to court.

7 The right to data portability and monetisation

The underlying element analysed in this study was the digital content trading system in the economy created by large digital platforms. The analysis covered specific content categories, i.e., user-provided, user-generated, or service-provider-generated content based on user data. Considering that such content often includes personal data and copyrighted content, a multi-level and cross-sectoral approach was taken to categorise and classify its definitions, and to establish legal protection issues. The term *user-provided private content* is a general representation of a dataset which includes non-copyrighted content. Making money on private content is a reality in many business models, and it poses numerous legal problems related to privacy, consumer law, and the harmonised approach to intellectual property law and e-commerce. The first issue was to determine which data could be included in the category of user-provided content and which could not. Combining the wording of the right to data portability from the GDPR with the wording of the Directive on the Supply of Digital Content and the Directive on Copyright and Related Rights in the Digital Single Market, it can be assumed that the "supplied data" include both data provided actively and passively (i.e., generated by cookies) while "data provided actively" can be both directly provided (i.e., sent by the user) and indirectly provided (i.e., by accepting the service provider's access to certain specified information). The concept of analysing the existing obligations concerning content portability and the possible measures to facilitate content transfer do not imply attaining the objective of improving the interoperability of services by imposing additional regulatory obligations. Besides, the transfer of one's own content (e.g., different types of files, messages stored in intermediaries' resources, etc.) and data (in the sense of the GDPR) from one provider of certain services to another and cross-border transfer are two different things, within the meaning of the "portability" regulation. In the latter case, access to content and the possibility to exercise, to some extent, the "portability" of that access are closely connected with copyright based on the territoriality criterion. This is also a critical element in proprietary rights. Recital 70 of that Directive states that the consumer could be discouraged from exercising remedies lacking conformity of digital content or a digital service if that consumer is deprived of access to content other than personal data, which he/she has provided or created through the use of the digital content or digital service. To ensure that the consumer benefits from effective protection regarding the right to terminate the contract, the trader should, therefore, at the request of the consumer, make such content available to the consumer following the termination of the contract.

The right to data portability applies to all "supplied" data. To define the objective parameters at the boundary between "active" and "passive" data, a "test" based on the following three variables has been proposed: the data subject's activity in providing the data, the data subject's awareness of providing the data, and the data controller's activity as regards collecting the data.

The sharing of actively provided data should be considered a legitimate form of barter payment in exchange for digital content. The legal protection of natural persons as regards managing user-provided private content covers the right to "transfer" such data from one data controller to another, which arises from the GDPR. However, it does not cover data other than personal data. Users should have the right to "license" such data if they are rightsholders (e.g., authors). As shown earlier in this paper, the "licensing" of user-provided content has already become a reality in the most popular social networks. Nonetheless, the statutory terms of service provision, covering the scope of "licensing," are too broad, and licences are granted to service providers in exchange for access to a particular community. The solution adopted under Article 7(4) of the GDPR, i.e., the right of data subjects to grant consent, is crucial in terms of regulating the issue of private content as a form of payment other than money. This is a user-centred system based on the users' control and awareness of managing "private content". Administration should be based on two separate legal tools: licences to use user-generated content and the right to withdraw and transfer such content from one platform to another, i.e., the full enforceability of the right to data portability (possibly in combination with the right to erase data). This awareness should be based on transparent information obligations regarding the commercial purposes of this data processing, in order to respect the principle of freedom of consent and the principle of purpose limitation (Malgieri, Custers, 2017:2). Recital 24 of the Directive concerning the supply of digital content reads as follows: "Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader". Such business models are used in different forms in a substantial sector of the market. While fully recognising that protecting personal data is a fundamental right, and, therefore personal data cannot be considered a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies. This Directive should, therefore, apply to contracts in which the trader supplies, or undertakes to supply, digital content or digital service to the consumer, and the consumer provides, or undertakes to provide, personal data. The personal data could be provided to the trader either at the time the contract is concluded or at a later date, e.g., when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service. EU law on the protection of personal data provides for an exhaustive list of legal grounds for the lawful processing of personal data. This Directive should apply to any contract in which the consumer provides, or undertakes to provide, personal data to the trader. For example, this Directive should apply when the consumer opens a social media account and provides a name and email address, which are used for purposes other than solely supplying the digital content or digital service, or complying with the legal requirements. It should equally apply when the consumer gives consent for any material which constitutes personal data, such as photographs or posts which the consumer uploads, to be processed by the trader for marketing purposes. Member States should, however, remain free to determine whether the requirements for the formation, existence, and validity of a contract under national law have been fulfilled. When digital content and digital services are not supplied in exchange for the payment of

a set price, the Directive should not apply to situations in which the trader collects personal data exclusively to supply digital content or digital service, or for the sole purpose of meeting the legal requirements. Such situations can include, for instance, cases in which the registration of the consumer is required by the applicable laws for security and identification purposes. The Directive should not apply to situations where the trader only collects metadata, such as information concerning the consumer's device or browsing history, except when this situation is considered a contract under national law. It should also not apply to situations in which the consumer, without having concluded a contract with the trader, is exposed to advertisements exclusively to gain access to digital content or a digital service (Recital 25 of the Directive).

If the consumer provides the entrepreneur with personal data, the entrepreneur should meet the obligations under Regulation (EU) 2016/679. These obligations are equally applicable if the consumer pays the fee and provides personal data. On termination of the contract, the entrepreneur should refrain from any further use of content other than the personal data provided or created by the consumer when using the digital content or digital service provided by the entrepreneur. Such content may include digital images, audio files, video files or content created using mobile devices. However, the trader should have the right to continue to use the content provided or created by the consumer if that content is not useful outside the context of the digital content or service supplied by that trader, if it relates solely to the activity of the consumer, if it has been combined with other data by the trader and cannot be separated from it, or such separation requires disproportionate effort, or if it has been generated jointly by the consumer and other persons, and can still be used by other consumers.

Yet, there is a sphere of content in which the data subject does not knowingly provide personal data but actively selects content (e.g., images contained in a specific folder) and shares those pieces to generate new data on an individual. Thus, determining the owner of such content becomes problematic. The question arises as to whether it is user data based on newly-produced content, or whether it becomes the property of the entity which allowed such content to be generated and bore the costs involved in this process. The conditions in which digital content is used often create uncertainty as to whether such content carries "shared" or "observed" data and whether the use of such data extends far beyond the activities involved in their generation.

One of the key issues related to digital content protection is identifying the need for establishing new ownership rights regarding raw and non-personal data as a common good. However, should such data be considered copyrighted digital content, it would be necessary to provide access to it to entities which are primarily public-interest oriented. Accordingly, permissible public use should include, for instance, the use of data in advanced research and content derived from the automated analysis of large datasets.

Consequently, these guidelines should be drafted with due regard for the general-interest objectives to be achieved through the measures taken by video-sharing platform providers and the right to freedom of expression. However, it seems that such a regulation should be left to Member States, which must consider not only the three-step test but also their national perception of the general-interest objectives (judgments passed in the following cases: C-120/78 Cassis de Dijon, C-33/74 Van Binsbergen, C-205/04 Gouda, C-76/90 Säger, C-384/93 Alpine Investments). For the mandatory requirements doctrine to be applied, a three-step test must be passed to demonstrate that (1) there is an overriding general (public) interest; (2) the measures implemented to pursue this interest are appropriate and adequate; and (3) the measures applied to implement that interest are proportionate. The protection of digital content created by Internet users can be achieved by making these platforms rely on the principles of interoperability , transparency, and openness. This concerns handling the digital content of network users.

8 Concluding remarks

8.1 Regulation of digital content

The problem of programming content regulation in the context of changes related to digitisation processes, the wide range of issues related to regulation in this sphere (e.g., digitisation of archival resources and the digital archiving of the programming portfolio of contemporary audiovisual media, the protection of children and young people on the Internet, the protection of privacy and the security of identity on the net, as well as the protection of intellectual property, and the combating of "network piracy"), and the reuse of public sector information – all these shape the digital media market. Its regulation will be the first context for new solutions related to regulating digital content on the net, especially concerning responsibility for digital content. This need for such regulation stems from the evolving digital processes and the inadequacy of current provisions in meeting the needs arising from the so-called digital revolution. What now appears indispensable is a general approach which will also define, in a systemic manner, the scope of protection related to digital content processing in an ICT network. This issue not only relates to services provided electronically and to the solutions proposed in the regulation on digital services but also concerns broadly understood inter-sectoral cooperation.

8.2 Level of regulations

It is worth pointing out that the objectives of the new regulations include improving the detection of illegal content on Internet platforms or creating a fast track to enable state authorities to contact the platforms and permanent contact points for service providers and state authorities (content policy). However, the convergence context makes it difficult to determine whether a given sphere of activity falls within the scope of arrangements only for digital services or whether it already goes beyond that and applies to the

regulation of infrastructure, i.e., those aspects of digital processes which are currently regulated at the EU level. Content regulation (digital content regulation, including the digitisation of archives and the legality of sharing) should be a matter of national solutions, considering the specificity of a given country and, in particular, national culture specificity. Therefore, it is of utmost importance to identify the spheres in which the national policy should apply, as this will consequently translate into governance and management in the digital field, i.e., the entire system of administration of a given Member State, to which a given field is subordinated.

8.3 Open character of digital resources

The purpose of digitisation is not only to protect collections from destruction or loss but also to share them. For this reason, the digital content accumulated by the Polish archives, libraries, and museums must not only ensure safe storage conditions but also be as widely available for users as possible, free of charge, and in a form which allows their reuse for non-commercial purposes. Pursuing the use of new technologies in preparing, securing, and sharing collections is the natural course of action for every institution taking care of its collections. This leads to the dispersion of digitisation initiatives, characteristic of all European countries, and results in the dispersion of digital content, making it difficult for users to access the resources they seek. Digital collections are created and stored by many institutions throughout this country, often as thematic virtual exhibitions, occasional publications, or resources only available locally on the computer terminals of the home institution. Using popular online search engines to search such dispersed resources not only fails to provide users with the complete picture of the digitised Polish cultural heritage but is also time-consuming and inconvenient. The sharing of digital collections online is regulated by the Act on Copyright and Related Rights of 4 February 1994, which stipulates that works for which the author's economic rights have expired, i.e., 70 years after the author's death, and for co-authors, after the death of the last surviving author, may be publicly disseminated without limitation (Article 36(1)). For digitised works, this restriction relates to both the authors and the translators or illustrators of the work. Article 28 of the Act on Copyright and Related Rights allows the permitted use for free sharing by libraries, archives, and schools of reproductions of works remaining under copyright protection, but only on the premises of such facilities, whilst the sharing by libraries, archives, and schools of digital reproductions on the Internet is no longer a permitted use within the meaning of that Act. This largely restricts the possibilities of sharing digital collections. Digital reproductions of copyright-protected documents are thus made available only at library computer stations. Therefore, the simple role of a digital library, which is online access to electronic resources not limited by time and place, is not fulfilled. In order to open the desired item (or at least verify it, if this indeed proves desirable), the reader must visit the library, even though the remote sharing of a digital reproduction would not be a technical problem. It is also essential to identify laws which could hinder the online sharing and reuse of publicly-owned cultural material. Unfortunately, Poland still lacks solutions to this problem. It should be emphasised that

exceptions to and limitations on copyright, including the principles of *fair use* and *fair dealing*, ensure an effective balance between the protection of authors in the scope of their creative activity, resulting from copyright or related rights, and the public interest. Such mechanisms guarantee certain privileges to users. This, in turn, opens up free space for action in the current copyright system. Given the rapid changes occurring in the field of technology and social behaviour, it is imperative to ensure the possibility of action using legally protected resources. Any restrictions on copyright, *fair use,* and *fair dealing* should be flexible and constantly adjusted to the needs and goals of the public interest.

It should also be noted that crucial questions have so far arisen about the limits of subjecting content to infrastructure regulation when the issue of market regulation is dominant. Yet, it seems there has been a new trend towards the reverse situation, whereby the regulation of infrastructure is subjected to digital content regulation. This also applies to the public sector and the information generated, stored, and processed there. Property rights can have an impact on restrictions pertaining to this subject. Such information, subject to the intellectual property rights of third parties, may not be reused. Therefore, the entity must refuse to reuse public-sector information if the intellectual property right does not belong to that entity or if it only has the right to use the work. Correspondingly, this applies to resources covered by legally protected secrets and to resources owned by network users, though they are not necessarily the subject of copyright or related rights.

One of the underlying problems concerning the regulation was the issue of determining whether public resources – public-sector information – are only those financed from public funds or also include resources which are owned by social organisations or natural persons but which have been made available to the public as part of the activities of public institutions. An important issue concerned determining whether the regulation should cover the sharing of national resources. This includes non-public collections, which are in the possession and at the disposal of public-sector institutions. The most crucial postulates of the groups involved regarding the provisions on reuse were the necessity to precisely define the scope of the public domain and to lift legal barriers in cases in which copyright and related rights could not be ascertained or in situations in which their owners were against it. However, the initiative of extending the provisions on reuse to cover all resources, including those under legal protection, requires the development of a new public policy on sharing public resources. The new reuse regulation does not address the above issues at the level of nation-states.

8.4 Social media regulation

The analysis of digital markets clearly defines the relationship between public authorities and the digital media environment. This is particularly true for an issue as troublesome as regulating digital content, including online media services. However, this view runs counter to the principle of the democratic will of the sovereign state, which pursues its own public interest, especially regarding cultural matters, when the equally fundamental

principles of subsidiarity and proportionality should be approached particularly seriously. Issues around regulating infrastructure and using tools for preventive content censorship are relevant, primarily because of the ever-changing shifts in the global position and role of market users. Technological advancements have increased the importance of infrastructure operators at the expense of content providers. This phenomenon is causing the entire digital world to be regulated at the technical and digital service access levels. This is why the service provider, or the digital service provider, is becoming so important. The examples of some countries prove the point that regulations adopted by public authorities in the field of digital media, whether more or less aggressive, are a means to strengthen the needs of the authorities, even in the most liberal areas. It is for this reason that public governance is today one of the main premises of public policy, including in the field of new technologies. As part of the planning process, the function of the public authority involves deciding on actions to achieve specific goals, and also redefining these goals by considering the requirements related to the development of modern technologies. All elements in advanced technologies, including software, digital services, and databases, exhibit the same characteristics, i.e., transfer rapidness (abrupt market changes in services, rapidly expanding technological innovations, especially in the context of network development, scientific research, etc.); globalisation (advanced technologies facilitating the global exchange of services in real time); entrepreneurship (the formation of cartels to conduct joint research for innovation, public-private partnerships); social participation (the development of innovative solutions by Internet users, the development of social media, crowdsourcing – the exchange of thoughts and concepts – all contributing to the growth in technology and innovations); convergence (combining multiple areas of human activity; technological convergence blurs the lines between individual fields in the legislative process, making it impossible to pinpoint threats and define liability through legislation, and to define the legal system alone), and result from freedom to exchange content. These characteristics also explain the need for changes and transformations related to establishing a new management system using legal instruments. Based on these important factors for developing new technologies, the case should be made to highlight the need to integrate the legal system in the most troublesome field of content regulation. Given the pace of technological and, in consequence, economic changes, this system must be characterised by flexibility, and the corresponding legal solutions should include universal standards allowing their application in different conditions and situations, depending on the nature of the digital content.

8.5 Legal security of digital content trading

Digital content has become a digital currency. This involves content created in the digital environment and that which has undergone digital conversion. It should be noted that this content may be subject to various kinds of protection. As regards determining the nature and legal status of digital content, on the one hand, a "test" is applied, which defines the following three elements: the data subject's activity in providing the data, the data subject's awareness of providing the data, and the data controller's activity in collecting

the data. On the other hand, to adequately protect user-provided content on the digital market, trading in such content should be based on three rules: the permission to use user-generated content, information obligations regarding content, and the right to withdraw and transfer such content from one platform to another. But, as in the case of personal data, the principle of exercising the right to transfer digital content, along with the right to erase such content (the demand to erase), should also apply. Legal transactions involving digital content should be based on transparent information for processing purposes, in order to control the principle of freedom of consent and the principle of purpose limitation. It is additionally essential to comply with the rule of transparency in business transactions on the ICT network. A key issue regarding the security of digital trading in digital content is determining the legal conditions under which "user-provided content" is protected in terms of copyright and the data subjects whose data is processed through various data-sharing platforms. This category of content may be subject to intellectual property protection within the framework, *inter alia*, of the Directive on Copyright and Related Rights in the Digital Single Market, as well as protection in terms of the subject-matter of e-services (e-commerce, in particular the proposed Digital Content Directive). The set of legal regulations referred to here is not uniform and is characterised by fragmentation in relation to specific sectors. For this reason, a cross-sectoral analysis appears indispensable to develop common definitions and options to manage user-provided private content on the digital market. The notion of user-provided digital content consists of several elements which should be taken into consideration in the context of the initiative in providing such content – the activities of the entity participating in its collection or processing and the extent of making use of such digital content by the platform user (which also includes taking into account third parties regarding the entity providing the data).

The convergence of digital media with traditional media has contributed to a special conflict which concerns defining the scope and level of the new regulations. This involves, in particular, digital content in which most issues touch on new media and new technologies (the protection of intellectual property, national identity, the right to privacy, and children and young people), as well as the economy (media market restrictions and the liability of digital service providers). New content management models (including online material) are emerging, accompanied by new rules for virtual organisation.

Evolution in communication technologies has materially changed the rules of the functioning of both individuals and societies. New multimedia platforms are being created to provide services electronically, which require modern technological solutions, usually financed by the private sector. An open and free global cyberspace allows cultural and experiential exchange across countries, societies, and individuals. It facilitates interaction and information sharing, leading to the spread of knowledge, experience, and technology. Freedom of speech and freedom of communication form the ideological grounds for such exchanges. The digital reality facilitates the performance of public tasks in a new social dimension (Chałubińska-Jentkiewicz, 2021:189).

The new technological order constitutes a premise and, simultaneously, the subject-matter of the discussed changes, which materially impact the regulatory area formed by digital media. Regulations applicable to this area of activities comprise four main aspects.

First, effective communication (i.e., freedom of speech as a fundamental right – Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Article 54 of the Constitution of the Republic of Poland, and Article 1 of the Press Law Act). According to T. Garton Ash, a free press is a distinctive feature of a free country, while censorship is a characteristic feature of a dictatorship. "A democracy cannot long survive without the former, a dictatorship without the latter" (Garton Ash, 2018:295). (One should stress that the issue of restrictions on the freedom of speech in a democratic system concerns decisions to interfere with the content of religious organisations, the owners of "free" media, political factions, and other social groups which adopt a strictly defined way of thinking – which is supported by digital media – thus enclosing themselves within **an ideological bubble.** This not only applies to the receipt of certain information by network users but also to sharing digital content. Philosopher Onora O'Neill was right to note that our media "must not only be accessible to but also assessable" (O'Neill, 2011, as cited in Garton Ash, 2018:301). However, as stressed by T. Garton Ash, "By rights, the most effective constraint on the media should be us, the readers, viewers, and users" (Garton Ash, 2018:379).

Second, political and cultural diversity (i.e., worldview pluralism) – this issue is discussed in the context of the public interest in the widely understood media space, in consideration of the rules of public morality and public interest, provided that the existing regulations are of a protective nature (for instance, Article 30 of the Treaty on the Functioning of the European Union, Article 31 of the Constitution of the Republic of Poland, and Article 18 of the Act on Radio and Television Broadcasting). This should also apply to the new regulations still lacking in the field of new digital media, which appear indispensable because of the arrangements regarding liability for shared digital content. The worldview pluralism and the global exchange of thoughts foster creativity and form significant elements in the development of societies while also serving the purpose of consolidating their classic bases, identity, and cultural diversity, which should be considered in any elements subject to future regulation. It should be noted that major opponents of pluralism and diversity in digital media are their owners (vast Internet platforms or media corporations). According to A. J. Liebling,"The freedom of the press is guaranteed only to those who own one" (Liebling, 1975:32), considering that "what we have in a one-paper town is a privately owned public utility which is Constitutionally exempt from public regulation, which would be a violation of the freedom of the press".

Third, regulations justified by economic reasons – this mainly concerns the market economy on a uniform digital market. The need for such solutions arises from the principle of the uniform application of competition rules across the European Union. The

issue of selecting the forms of digital media market regulations, resulting from Poland's membership in the European Union, appears crucial in this context. Therefore, in the vast majority, these are EU regulations forming the basis for analysing documents, directives, and proposals defining a given regulatory area. According to the above-cited A. J. Liebling, "The function of the press in society is to inform, but its role in society is to make money" (Liebling, 1975:32). This rule can serve to define the purposes of the currently operating large Internet platforms.

On the one hand, they constitute an example of fragmentation and concentration which, to a great extent, results from binding self-regulatory principles. On the other hand, they are an efficient model of making money by exchanging user data, digital content, and databases without generating excessive costs still incurred by traditional media in connection with pluralism and objectivism. Digital platforms cannot be assumed to provide thorough information justifying their functioning. Driven by the rule that comments cost nothing while facts cost a lot, they have no intent to bear editorial responsibility for shared digital content, the verification of which is rather expensive.

Fourth, public service (i.e., the public interest and its objectives in the digital media sector), which in particular requires redefining objectives and orienting regulations towards ensuring the broadly-defined cybersecurity (including the need for protecting against disinformation, the violation of the right to privacy, hate speech, and content harming public morality, as well as safeguarding national identity, sovereignty, and the raison d'état of individual countries).

It is worth noting here that traditional media, in pursuing their public mission, begin to lose significance when faced with the omnipotence of social media, in which network users publicise content for other users without any in-depth analysis of what fulfilling public duties in media really is. Neither are such discussions conducted by those entities for which the media serve the purpose of implementing their diverse objectives, which are not related to any public interest.

The role of a nation-state – as borders no longer seem to matter in the global network context – is visible and fulfillable (at least to some extent) at each level, jointly forming the regulatory area of new digital media. The digital era has triggered the need to analyse the regulations applicable in this entire sphere. It appears necessary to modify the current forms of ***public authority*** as regards protecting public interest. This results from the fact that not all the executive instruments currently applied in the traditional approach to public administration duties (restrictions – registers, concessions, rules of territorial jurisdiction, and even the basic implementation of the legal regulations applicable to new digital media, e.g., cybercrime prosecution or editorial responsibility) are practicable in the new digital environment, which shapes not only a range of social behaviours and attitudes but also a new quality of the relationship between the state and individuals. Redefining public interest in this new and unregulated world should be coupled with

searching for new instruments to protect that interest and establishing new responsibility rules for shared digital content.

The business of digital content providers consists of making content available through information and communication systems. This category is highly diverse. It includes 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 the active form of their operations online, content providers bear direct liability for any breaches caused by such operations.

In Poland's legal system, content providers are directly liable for infringements of third-party rights. As noted by J. Barta and R. Markiewicz, controversies arose around attempts at qualifying the issue of making works available in computer networks (Barta, Markiewicz, 2001:228). Ultimately, this was qualified as a new field of commercialisation, i.e., making a work available in a manner that it could be accessed by anyone at any time and place they choose. This issue was highly relevant for ICT networks whose functioning was based on interactivity. As a result of digital processes, users can modify and share content without problems. The concept of *sui generis* protection of content producers' or providers' rights appears interesting. It was discussed at the *Association Littéraire et Artistique International* (ALAI) congress in 1996, with attempts to formulate a construct allowing producers to claim protection against third parties. Among others, consideration was given to affording them the status of moral rights or quasi-moral rights, with the caveat that they might not have limited the moral rights of content creators (Dietz, 1997; as cited in Gęsicka, 2014:290). According to J. Barta and R. Markiewicz, the construction of these rights is similar not to moral rights but to the author's economic rights (Barta, Markiewicz, 2001:228). It was this core objective, primarily economic, that these entities had in view, bringing these rights closer to related rights.

Table 1: Public interest in the new media v. New risks

Public-interest objectives in the media as presented to date	**New threats connected with the development of digital media**
protection of pluralism and opinion diversity	digital divide
protection of national and European culture from the domination of mass culture	new type of social exclusion
protection of children and young people	weakening of citizenship, cultural and national identity
protection of human dignity, no discrimination	cybersecurity
consumer protection	weakening of the right to privacy and lack of anonymity
	infringement of the ownership right (copyrights to digital content, databases)
	loss of data confidentiality
	information war and disinformation

When talking about the changes being brought about by new technologies in the digital content-sharing environment, we must remember that this development requires an interdisciplinary approach, combining the knowledge and experience of experts in the fields of economics, sociology, technology, the media, political science, psychology, culture, and security science. Today's living conditions largely depend on the state of the information and communication technologies functioning in a given country. We are currently witnessing radical changes both in how societies function and in the global economy because of the expected spread of innovative information and communication solutions. Freedom of speech and freedom of communication form the ideological grounds supporting such exchanges. Thanks to new mass media technologies (ICT networks, the Internet) – a subject that has been explored particularly extensively – entirely new and previously unknown approaches to family, professional, and public life have emerged. Along with the development of digital technology and social changes, including those associated with forming the so-called digital democracy, new fields of human action have emerged, commonly described as the ICT network environment, and more broadly understood as cyberspace. They affect all aspects of human life. The same is true for social and economic relations, and the state-individual accord, which includes exercising fundamental human rights. The digital revolution we are witnessing, including, in particular, automated data-processing technologies, which affect human-related decision-making processes, takes us back to the questions about human rights and freedoms. Whereas regulatory restrictions previously applied to the relations between the state and the individual, current normatively enshrined steps taken by public authorities are becoming a means to protect the rights and freedoms of individuals first and only then to ensure public security, order, and morality, in a world driven by technology used for a wide range of purposes, except that behind each *technē*, even the most automated, there

is a person. Aristotle (384–322 B.C.) maintained that a distinction should be made between *technē* (practical skills, art) and *epistēmē* (scientific insights, knowledge) (Aristotle, 2005:114, translated by Piotrowicz). According to this philosopher, knowledge forms include all sciences, while art and practical skills represent inferior occupation types associated with craftspeople and slaves. According to this concept, *technē* is an obstacle to practising virtue in the souls and minds of the free. This historical approach related to contempt for *technē*, which is usually not associated with such notions as ethics, public morality, or personal interests, continues to be relevant, especially in the context of the right to privacy, the protection of personal interests, and moral standards (Chałubińska-Jentkiewicz, Karpiuk 2015: 6). In the field of modern technology, there is an ongoing conflict between them and so-called sensitive interests. An open and free global cyberspace allows cultural and experiential exchange across countries, societies, and individuals, facilitating interaction and digital content sharing, and leading to the exchange of knowledge and experiences. Hence, it can be said that digital content sharing facilitates the exchange of technology, thereby driving innovation. The development of new technologies and the associated processes of social changes require a new regulatory approach and a redefinition of public-interest objectives and public-authority responsibilities in the process of regulating the areas which are relevant to the core aspects of the functioning of the individual – citizens, markets, and states. Convergence processes occurring in so far differently understood regulatory areas contribute to the rise of a special type of conflict as to the scope and level of new regulations. Difficulties arise in specific globalisation conditions, exterritorial digital services, and due to the absence of universal state jurisdiction and sovereignty rules.

In the modern-day cyberspace realm where individuals function, it seems necessary to establish norms and, before this, rules and values to apply as standards in the real world. Freedom in the online environment also requires security and protection and, consequently, regulatory restrictions. However, due to the nature of cyberspace, new needs must be considered. This includes establishing new values, also those specific to that environment. This is particularly evident when most of our activities have moved to the online realm due to the COVID-19 pandemic. In particular, this applies to defining the roles of Internet users and the rules of liability for online activities. Yet, this is only one piece of the highly complex issue of advanced-technology development in the context of the legislative process, affecting almost every state, society and the weakest of all links – the individual.

The state must gradually limit the scope of its governance function in favour of shaping development, standardisation, and mediation strategies and mechanisms. An important part of this function is to make projections about forecasts. This requires an extensive analysis of local and global considerations, economic, social, and political needs and interests, and the possibility of meeting individual needs. A diagnosis and strategy would help to formulate the appropriate regulatory policy, which is closely linked to the realm of governance. The sphere of development governance differs from the other three areas

of public administration functioning in that it is oriented more towards the future functioning of the state. It is for this reason that governance is now one of the central premises of public policy, including new technologies. To take these measures, public authorities need norms. These revolutionary changes involve state government (including the entire e-government area), chiefly because previous state government and governance methods will prove ineffective in a society where information has become the main instrument and digital content – the primary product. Modern technologies have created administrative convergence – a process whereby new, common administrative solutions are developed to replace traditional administrative divisions. These areas are usually defined at the EU level. They are divided along the lines of new threats to the rights and freedoms of individuals – and to the European Economic Area. One of the key regulatory objectives in the legislative process is to guarantee cybersecurity, which requires the accessibility and integrity of networks and infrastructures, and also, most importantly, the confidentiality of digital data processed within them and their ownership protection, as well as their security against illegal content. This means that protecting the fundamental rights and freedoms of individuals sets the bounds within which each legislative process should take place. This also applies to drafting legislation due to the development of new media, including social media. Freedom of speech and the right to communication are not absolute values, and, as such, they represent no obstacles to regulations geared towards the public interest, security, public order, public morality, and the rights and freedoms of other individuals (Article 31(3) of the Constitution of the Republic of Poland).

All elements in advanced technologies, including software, services, databases, and equipment, exhibit the same characteristics, i.e., rapidity (abrupt market changes in digital services, rapidly expanding technological innovations, especially in the context of Internet development, data processing (automatic profiling), etc.); globalisation (advanced technologies facilitating the global exchange of digital services on the digital market in real time); entrepreneurship (the formation of consortia to conduct joint research for innovation, public-private partnerships); social participation (the development of innovative solutions by Internet users, the growth of social media, crowdsourcing – the exchange of thoughts and concepts – all contributing to the growth in technology and innovations); convergence (combining multiple areas of human activity; technological convergence blurs the lines between individual fields of the legislative process, making it impossible to pinpoint threats and define liability through legislation, and to define the legal system alone). These characteristics explain the need for changes and transformations related to establishing a new system for digital content management using legal instruments. Based on these important factors in developing new technologies, a case should be made to highlight the need to integrate the legal system in cyberspace.

The assessment of the digital markets in the above-mentioned scenarios – for instance, based on Freedom on the Net reports – clearly defines the relationship between public authorities and the digital media environment. This is particularly true for an issue as

troublesome as regulating electronic media content, including online digital services. However, this view runs counter to the principle of the democratic will of a sovereign state, which pursues its own public interest when the equally fundamental principles of subsidiarity and proportionality should be approached particularly seriously. Issues around regulating the operations of digital service providers (as in the case of editorial responsibility and publisher's liability) and using tools for preventive censorship in digital content are relevant primarily because of the ever-changing shifts in the global position and roles of market users. Technological advancements have increased the importance of infrastructure operators – or, more specifically, content distribution platforms – at the expense of the providers of the same content. This development leads to the entire digital world being regulated at the technical and network organisation access levels. Some examples of the proposals for digital market regulations discussed in this treatise prove that regulations adopted by public authorities in cyberspace, whether aggressive or not, are ways to strengthen authorities' needs, even in the most liberal areas. This is particularly relevant as the digital content-sharing world is in growing need of regulations.

References:

Angelopoulos, C. & Smet, S. (2016) Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability, *Journal of Media Law*, 8(2), http://dx.doi.org/10.2139/ssrn.2944917.

Barta, J. & Markiewicz, R. (2001) *Internet a prawo* (Warszawa: Wydawnictwo Universitas).

Chałubińska-Jentkiewicz, K. & Karpiuk, M. (2015) *Prawo nowych technologii. Wybrane zagadnienia* (Warszawa: WoltersKluwer).

Chałubińska-Jentkiewicz, K. (2021) *Prawne granice dezinformacji w środkach masowego przekazu* (Toruń: Wydawnictwo Adam Marszałek).

Cooter, R. & Ulen, T. (2011) *Law & Economics* (Boston: Addison-Wesley).

Dietz, A. (1997) General Report, In: Dellebeke, M. (ed.) *Copyright in Cyberspace* (Amsterdam: Otto Cramwinckel).

Frosio, G. & Mendis, S. (2020) Monitoring and Filtering: European Reform or Global Trend?, In: Frosio, G. (ed) *The Oxford Handbook of Online Intermediary Liability* (Oxford: Oxford University Press).

Galloway, S. (2018) *Wielka czwórka. Ukryte DNA: Amazon, Apple, Facebook i Google* (Poznań: Wydawnictwo Rebis).

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

Geere, D. (2012) *How deep packet inspection works*, available at: https://www.wired.co.uk/article/how-deep-packet-inspection-works (October 4, 2024).

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

Horten, M. (2016) *The Closing of the Net* (London: Polity Press).

Liebling, A. J. (1975) *Wartość liczbowa odnośnie do rywalizujących gazet codziennych New Yorker* (New York: New Yorker).

Lucas, E. (2017) *Oswoić cyberświat. Tożsamość, zaufanie i bezpieczeństwo w internecie* (Warszawa: Kurhaus Publishing).

Ombelet, P. J., Kuczerawy, A. & Valcke, P. (2016) *Employing Robot Journalists: Legal Implications, Considerations and Recommendations* (Montreal: The Web Conference), pp. 731-736.

Rossi, A. (2020) *After Truth: Disinformation and the Cost of Fake News*, available at: https://www.youtube.com (February 17, 2021).

Saba Bebawi, S. & Bossio, D. (2014) *Social Media and the Politics of Reportage: The 'Arab Spring'* (London: Palgrave Macmillan London), pp.1-8.

Based on the #Digital2020 report, available at: https://mobirank.pl/2020/02/23/digital-mobile-i-socialmedia-w-polsce-w-styczniu-2020-roku (July 20, 2020).

Urban, J., Karaganis, J. & Schofield, B. (2016) Notice and Takedown in Everyday Practice, *UC Berkeley Public Law Research Paper*, No. 2755628, https://dx.doi.org./10.2139/ssrn.275562.