Santander Art and Culture Law Review 2/2020 (6): 279-292
DOI: 10.4467/2450050XSNR.20.020.13023

LEGAL COMMENTARIES

Katarzyna Chałubińska-Jentkiewicz*

k.jentkiewicz@akademia.mil.pl
orcid.org/0000-0003-0188-5704
Department of Cybersecurity Law and New Technologies Law
Law Institute
War Studies University
al. gen. A. Chruściela „Montera" 103
00-910 Warsaw, Poland

Digital Single Market. Cyber Threats and the Protection of Digital Contents: An Overview

Abstract: Access to audio-visual and digitized heritage is crucial for the economy and overall well-being. It also offers important avenues for the development of creativity and intercultural dialogue, shaping people's identity and contributing to cultural diversity. Yet the rise of the digital sector has also been accompanied by the proliferation of cyber or computer-related crime. Therefore, the harmonization of cybercrime legislation has widely been discussed in different international fora. At the same time, the protection of digital content has become a highly important issue in the context of the expanding policies aimed at ensuring public, open access to digitized resources for non-commercial, educational, and cultural purposes. This article offers an overview of these topical questions, with specific reference to the EU Digital Single Market.

* **Katarzyna Chałubińska-Jentkiewicz** is Associate Professor and Chief of Department of Cybersecurity Law and New Technologies Law at the Law Institute of the War Studies University in Warsaw, Poland. She also serves as Director of the Academic Centre for Cybersecurity Policy at this university. She is a member of the Digitization Council (for the term 2019-2021) at Poland's Ministry of Digital Affairs. In 2011-2017, she served as Deputy Director of the National Audio-visual Institute, a public institution responsible for digitization and the dissemination of audio-visual heritage. Her research expertise covers cyber security, the law of new technologies, information security, development of electronic media, protection of intellectual property, and digitization.

The author wishes to acknowledge that this article has been prepared as a result of cooperation in realization of the research project, entitled "The Polish Cybersecurity System – A Model of Legal Solutions" (Agreement MON No. GB/4/2018/208/2018/DA), granted by the Ministry of National Defence.

Katarzyna Chałubińska-Jentkiewicz

Keywords: cyber threat, digital content, digital heritage, consumer rights, intellectual property

Introduction

New communication technologies – especially nowadays in times of a global pandemic – are of key importance not only for economic and social growth but also for cultural development. Not only do these enable people-to-people contacts, but they also facilitate access to culture and heritage at a time when cultural institutions are closed down or restricted in terms of their pre-Covid-19 activities. In fact, "[t]he outbreak of the Covid-19 pandemic particularly threatens the future of artists, creators and cultural operators, who are severely impacted by the enforcement of social distancing measures and the consequent postponements, cancellations or closures of events, live performances, exhibitions, museums and cultural institutions".[1] While the whole creative sector has been deeply affected by lockdown measures, the audio-visual industries are fighting back during this current crisis. Many cultural events, spectacles, and art exhibitions have moved online, and a number of support measures have recently been launched by both public and private institutions, governments, and regional organizations, such as the European Union (EU).[2]

The significance of a wider access to culture, to audio-visual and digitized heritage, and to digital content more generally is undeniable for the economy and people's well-being, offering "broadened opportunities for creation, communication and sharing of knowledge among all peoples".[3] At the same time however, the digital sphere is greatly affected by illicit practices and crimes, which also concern the cultural and audio-visual sectors, including *inter alia* the infringement of intellectual property rights.

While referring to the EU Digital Single Market, this article offers an overview of these topical questions. First it explains how the law and legal scholarship identify computer crime or computer-related crime or cybercrime. Next it briefly scrutinizes the notion of "digital content", and explains the scope of its protection. The article then concludes with a set of observations on the new boundaries of responsibility for digital content.

[1] M. Pasikowska-Schnass, *EU Support for Artists and the Cultural and Creative Sector During the Coronavirus Crisis*, May 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649414/EPRS_BRI(2020)649414_EN.pdf [accessed: 20.10.2020].

[2] For instance, see F.J. Cabrera Blázquez et al., *The European Audiovisual Industry in the Time of COVID-19*, European Audiovisual Observatory, Strasbourg 2020.

[3] Charter on the Preservation of Digital Heritage, 15 October 2003, http://portal.unesco.org/en/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html [accessed: 18.10.2020].

Defining Computer Crimes

Originally, the term "computer" crime was understood in two ways.[4] First, computer-related offences were defined as a group of acts that boiled down to using a computer to violate any legal right protected by criminal law. Secondly, the term was used to describe offences that were committed by people with high skills and knowledge of electronics or computer science. In this latter approach the perpetrator's possession of specific knowledge and skills was treated as an important element of computer crime.[5] For this reason usage of the term "IT crime" has also been suggested, since it would refer directly to a scientific discipline dealing with information-processing technologies as well as with technologies producing information processing systems.[6]

Criminologists as well as dogmatists of criminal law have repeatedly tried to strictly define crimes committed with the use of modern computer technology. Accordingly, computer crime has been defined as a forensic phenomenon covering all criminal behaviour related to the functioning of electronic data processing, directly harming processed information, its owner, carrier, and object in a computer and in the entire computer connection system, and the computer hardware itself as well as the rights to computer software.[7] It has also been deemed to refer to acts bringing about losses, harm, or damage with respect to the purposes for which data processing systems have been used.[8] In this regard, one of the most influential and comprehensive scholarly definitions of computer crime was proposed by Donn B. Parker, a world-famous US security researcher in his *Computer Crime: Criminal Justice Resource Manual* (first published by the US Department of Justice in 1980, and reprinted in 1989).[9] Accordingly, computer-related crimes were defined in a broader sense as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution".[10]

---

4 See S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*, December 2008, pp. 2-9, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf [accessed: 20.10.2020].

5 For an overview of the notion of computer-oriented crime, also see M.F. Miquelon-Weismann, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, "John Marshall Journal of Computer and Information Law" 2005, Vol. 23(2), pp. 330-334.

6 See D.A. Jenks, J.R. Fuller, *Global Crime and Justice*, Routledge, London–New York 2016, p. 174; M. Siwicki, *Cyberprzestępczość* [Cybercrime], C.H. Beck, Warszawa 2013, p. 10.

7 K.J. Jakubski, *Przestępczość komputerowa – podział i definicja* [Computer Crime – Classification and Definition], "Przegląd Kryminalistyki" 1997, Vol. 2, p. 31; see also H.J. Schneider, *Kriminologie*, De Gruyter, Berlin–New York 1987, p. 48.

8 See B. Hołyst, *Kryminalistyka* [Forensic Science], 8th ed., Wydawnictwa Prawnicze PWN, Warszawa 1996, p. 241, citing earlier works by D.B. Parker.

9 D.B. Parker, *Computer Crime: Criminal Justice Resource Manual*, 2nd ed., National Institute of Justice, Washington DC 1989.

10 Ibidem, p. 2.

On the other hand, the definition adopted by the Committee of Experts of the Organization for Economic Cooperation and Development (OECD) in 1986 considered computer-related crime "as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data".[11] The considerable generality inherent in this definition proved to be very useful, because it did not limit its application when technological and legal changes occurred.

The first institutional initiative on a computer crime in Europe was the conference of the Council of Europe (CoE) on criminological aspects of economic crime in 1976, when several categories of computer crime were discussed.[12] The next important step in defining computer crime was taken by a group of experts of the CoE and resulted in a report,[13] subsequently endorsed by Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime.[14] This soft law instrument recommended that the CoE's Member States introduce to their criminal codes provisions prohibiting and penalizing several acts listed in the expert report. These acts included: computer-related fraud; computer forgery; damage to computer data or a program; computer sabotage; unauthorized access; unauthorized interception; unauthorized reproduction of a protected computer program or data; unauthorized reproduction of a topography (a minimum list); alternation of computer data or computer programs; computer espionage; unauthorized use of a computer; and unauthorized use of a protected cultural program (optional list). In turn, the following CoE Recommendation of 1995[15] referred to "computer-related crime", considered as any crime in which the investigating authorities must gain access to information processed or transmitted in computer or electronic data processing systems.[16] Importantly, in an appendix it offered a set of principles on criminal procedural law connected with information technology which Member States should take into account when reviewing their internal legislation and practice.

With the rapid development of computer technologies and computer networks in the late 1990s, the problem of cyberthreats greatly grew in prominence and the search for a closer system of global cooperation to suppress it became pressing.

The draft International Convention on Cybercrime and Terrorism, developed by Stanford University in 2000, defined cybercrime as "conduct, with respect to

11 See S. Schjolberg, op. cit., p. 8.

12 European Committee on Crime Problems, *Criminological Aspects of Economic Crime: Reports Presented to the Twelfth Conference of Directors of Criminological Research Institutes (1976)*, Council of Europe, Strasbourg 1977.

13 See European Committee on Crime Problems, *Computer-Related Crime*, Council of Europe, Strasbourg 1990.

14 13 September 1989.

15 Council of Europe, *Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology*, 11 September 1995.

16 J. Kosiński, *Paradygmaty cyberprzestępczości* [Cybercrime Paradigms], Difin, Warszawa 2015, p. 38.

cyber systems, that is classified as an offense punishable by this Convention" (Article 1(1)).[17] In turn, the 2001 communication from the European Commission described computer crime "in the broadest sense, as any crime that in some way or another, involves the use of information technology".[18] This document distinguished between crimes related to a given computer and traditional crimes committed by means of computer technology.[19]

On the level of international law, the most important notions are to be found in the Convention on Cybercrime,[20] adopted, also within the CoE's framework, in 2001. This instrument seeks to address computer crime by standardizing and harmonizing national laws, improving investigative techniques, and increasing cooperation among States. As of October 2020, 65 States are party to this Convention, including the vast majority of EU and CoE Member States, and such non-European technological powers as Canada, Israel, Japan, and the USA.

The Convention on Cybercrime, in its Articles 2-9, offers a catalogue of offences related to the use of computers. In particular it defines two computer-related offences: "computer-related forgery" (Article 7) and "computer-related fraud" (Article 8). The purpose of the first article was "to create a parallel offence to the forgery of tangible documents", while the aim of the latter provision was "to criminalize any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property".[21] In turn, Article 10 of this Convention regards offences related to infringements of copyright and related rights. Not surprisingly, the criminalization of infringement of copyrights is particularly important for the creative, artistic, and audio-visual sectors, where "protected works include literary, photographic, musical, audiovisual and other works".[22]

EU legislation on cybercrime, which is based on its competence in judicial cooperation in criminal matters,[23] corresponds to the rules set out in the CoE's Convention on Cybercrime.[24] Insofar as concerns national legislation in this regard,

[17] A.D. Sofaer et al., *A Proposal for an International Convention on Cyber Crime and Terrorism*, August 2000, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf [accessed: 15.09.2020].

[18] European Commission, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime"*, 26 January 2001, COM(2000) 890 final, p. 12.

[19] J. Kosiński, op. cit., p. 41.

[20] 23 November 2001, ETS No. 185.

[21] See Council of Europe, *Explanatory Report to the Convention on Cybercrime*, 23 November 2001, ETS No. 185, paras. 81 and 86.

[22] Ibidem, para. 107.

[23] See Article 83(1) of the Treaty on the Functioning of the European Union, consolidated version: OJ C 202, 7.06.2016, p. 47.

[24] See European Commission, *Cybercrime*, https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en [accessed: 20.10.2020].

anti-cybercrime provisions are usually scattered across many and various laws and regulations. For instance, in the Polish legal system computer crime is not regulated under one single piece of legislation. Provisions regarding offences of this kind can be divided into two basic groups: those regulated under specific parts of the Polish Criminal Code,[25] and those normalized under the criminal provisions of individual Acts. In the latter regard, the provisions of the Act of 4 February 1994 on Copyright and Related Rights ("Copyright Act")[26] are of particular relevance. Accordingly, a computer software program is subject to copyright in the same way as any other work within the meaning of this Act. The infringement of this protection is subject to the criminal sanctions set forth in the Copyright Act. Importantly, protection is granted to all programs that fulfil the conditions set out in the Act, i.e. that are manifestations of creative activity of an individual nature and that are established in any form. The purpose of the computer software and its value are irrelevant, because the law guarantees the authors of such works protection analogous to that of authors of literary works. In addition, given their specific nature as well as the ease of copying and distributing, several regulations which increased their protection against computer piracy have been adopted.[27]

Digital Content, Intellectual Property Rights, and the EU Digital Single Market

Another important concept for assessing cyber responsibility in the context of the issue of protection, and what problems may arise from its definition, is that of digital content. In addition, when referring to the market for digital services and responsibility for their provision, the concept of "digital content" is the basic term that requires definitional clarification.

While referring to EU law and policy, the European Commission announced in May 2015 "A Digital Single Market Strategy for Europe",[28] based on three pillars: access to online products and services; conditions for digital networks and services to grow and thrive; and growth of the European digital economy. That same year the definition of "digital content" was also proposed in the draft of the Directive

[25] See *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny*, consolidated text: Dz.U. 2020 item 1444, as amended.

[26] *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych*, consolidated text: Dz.U. 2019 item 1231, as amended.

[27] See further M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne* [Cybercrime – Definitions and Legal Provisions], "Biuletyn EBIB" 2010, Vol. 4, http://www.ebib.pl/2010/113/a.php?nowak [accessed: 29.04.2020].

[28] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "A Digital Single Market Strategy for Europe"*, 6 May 2015, COM(2015) 192 final.

of the European Parliament and of the European Council on certain aspects of contracts for the sale of goods concluded via the Internet or otherwise in a remote manner.[29] According to this definition, "digital content" means "data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software"; "a service allowing the creation, processing or storage of data in digital form, where such data is provided by the consumer"; and "a service allowing sharing of and any other interaction with data in digital form provided by other users of the service" (Article 2(1)). Yet the final version of Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services[30] offers a much more concise definition (Article 2(1)). Accordingly, "'digital content' means data which are produced and supplied in digital form", thus encompassing a wide range of data, including those important for cultural heritage, such as e-books, files with music, movies, photos, etc.

The distribution of digital content in the network through audio-visual media services is by definition characterized by a cross-border nature. Their producers, creators and their heirs, and most of all the recipients – consumer service users – benefit from it. The processes of digitization and the sharing of digital content in a global way contribute to increasing access to reliable sources of knowledge and resources that may have been forgotten, including those remaining in the public domain as well as new resources created on the basis of archives.

As already indicated, the protection of intellectual property constitutes a key issue for the development of new technologies. This type of protection denotes an extremely important developmental aspect connected not only with the features of creative work itself in many areas of human activity, but also with a strictly-defined material and moral benefit belonging to the entities entitled to them on account of ownership. It is no doubt a truism to say that the protection of intellectual property has an economic aspect.[31]

Intellectual property is closely related to the processes of creation, development, and use of acquired knowledge, and is also the result of human creativity and the creativeness involved in all inventions that are the subject of business trading. Hence on the one hand there is the media industry and the audio-visual market for media services, and on the other the market for services related to the distribution and all other uses of digital content.

[29] European Commission, *Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content*, 9 December 2015, COM(2015) 634 final – 2015/0287 (COD).

[30] OJ L 136, 22.05.2019, p. 1.

[31] See Article 2(viii) of the Convention Establishing the World Intellectual Property Organization (WIPO), 14 July 1967, as amended on 28 September 1979, 828 UNTS 3.

In December 2015, the European Commission issued a communication entitled "Towards a Modern, More European Copyright Framework".[32] In this document the Commission indicated three objectives of the necessary regulation: (1) supporting the efforts of the copyright holders and distributors to reach an agreement on licenses that allow cross-border access to digital content (the instruments to achieve such goals are to be mediation and similar alternative mechanisms of resolving possible disputes); (2) facilitating the digitization of works not available on the market and making them available throughout the entire EU; and (3) increasing the cross-border distribution of television and radio programmes. In the context of the scope of permitted public use, the Commission identified three areas of regulatory intervention: the cross-border use of digital content in education; in the field of scientific research; and for the purpose of preserving cultural heritage.

The aforementioned objectives have subsequently been introduced into the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market.[33] As regards the availability of audio-visual works on the video-on-demand platforms, the rule that is applied is based on using the mechanism of conducting negotiations, which requires development at the level of a Member State. In relation to the content remaining outside commercial circulation, the principle of extending the scope of negotiations to all – and not only to selected – works of this type has been adopted. In the case of using works and other objects protected in digital and cross-border teaching activities, some freedom is left to a Member State, which may decide on the permitted public use depending on the possibility of obtaining a license. In the case of using digital content for research purposes, the possibilities of free use are be limited to a specific group of entities. In turn, with respect to activities related to the protection of cultural heritage a rule has been introduced consisting of a mandatory provision of copies of the work to cultural heritage institutions for the purpose of the safekeeping of their content.[34]

At the same time it should be noted that the application of exceptions to the need to obtain a permit as specified in the Directive is limited to only a few situations. The use of a digital content must relate to: (i) works carried out by scientific

[32] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Towards a modern, more European copyright framework"*, 9 December 2015, COM(2015) 626 final.

[33] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.), OJ L 130, 17.05.2019, p. 92.

[34] According to the 13th Recital of Directive 2019/790: "Cultural heritage institutions should be understood as covering publicly accessible libraries and museums regardless of the type of works or other subject matter that they hold in their permanent collections, as well as archives, film or audio heritage institutions. They should also be understood to include, inter alia, national libraries and national archives, and, as far as their archives and publicly accessible libraries are concerned, educational establishments, research organizations and public sector broadcasting organization".

research institutions for scientific purposes (Article 3); (ii) text and data mining of reproductions and extractions of lawfully accessible works and other subject matter (Article 4); (iii) the use of works and other subject matter in digital and cross-border teaching activities (Article 5); and (iv) the preservation of cultural heritage (Article 6). In this latter regard:

> Member States shall provide for an exception [...] in order to allow cultural heritage institutions to make copies of any works or other subject matter that are permanently in their collections, in any format or medium, for purposes of preservation of such works or other subject matter and to the extent necessary for such preservation.

Importantly, under Article 8 of Directive 2019/790 rules have been introduced for the use of out-of-commerce works and other subject matter by cultural heritage institutions. It needs to be noted that the role of these institutions is seen as crucial not only for the development of the cultural sector, but also for innovation in such sectors as learning and tourism.[35] Hence, pursuant to Article 8(1) of Directive 2019/790 Member States are obliged to:

> provide that a collective management organization, in accordance with its mandates from rightholders, may conclude a non-exclusive licence for non-commercial purposes with a cultural heritage institution for the reproduction, distribution, communication to the public or making available to the public of out-of-commerce works or other subject matter that are permanently in the collection of the institution, irrespective of whether all rightholders covered by the licence have mandated the collective management organisation.

There are two conditions for such a non-exclusive licence for non-commercial purposes: "the collective management organization is, on the basis of its mandates, sufficiently representative of rightholders in the relevant type of works or other subject matter and of the rights that are the subject of the licence"; and "equal treatment is guaranteed to all rightholders".

Moreover, under Article 8(2) of Directive 2019/790, Member States shall "allow cultural heritage institutions to make available, for non-commercial purposes, out-of-commerce works or other subject matter that are permanently in their collections", provided that "the name of the author or any other identifiable rightholder is indicated, unless this turns out to be impossible", and that "such works or other subject matter are made available on non-commercial websites". However, all rightholders may at any time request that the protected objects be considered

[35] See the 65th Recital of the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.06.2019, p. 56; also see A. Wallace, E. Euler, *Revisiting Access to Cultural Heritage in the Public Domain: EU and International Developments*, "IIC – International Review of Intellectual Property and Competition Law" 2020, Vol. 51, pp. 851-852.

works in business circulation and exclude the use of licences (Article 8(4)), and the rights of rightholders from third countries must be respected (Article 8(7)). In the case of cinematographic or audiovisual works, the regulations of the third country in which the seat or permanent residence of the producer is located shall be applicable. Recital 27 of the Directive indicates that digitization projects may involve significant investments, therefore it is assumed that cultural institutions as copyright holders may generate revenues from the granting of licences based on the mechanisms discussed here to cover the costs of licences and the costs of digitization and the dissemination of works.

The legal interpretation of the provisions indicated above seems obvious when it comes to the regulations regarding content transmitted as part of audio-visual activities. However, doubts arise when one asks the question which audio-visual policy issues are applicable within the scope of cultural activities, including digital content (as well as their protection and terms of transmission), when one takes into account such values as public morality, national identity, or other goals in the public interest, implemented also as part of the media market regulation; i.e. which should remain within the competence of the Member States themselves, and to what extent certain elements of audio-visual policy, constituting part of the Digital Single Market, should remain subject to the EU conceptualization.

Convergence of the means of social communication makes one wonder how the system allocating legal ownership and responsibility should be shaped in a situation when the traditional roles of its users begin to interpenetrate. It should be noted that in legal and policy instruments referring to copyright issues, the EU law maker uses the concept of a work or content, while the scope of the current regulations in the Digital Single Market cover a broader context, which also includes infrastructure (hardware) as well as digital content and digital services (software). So far, important questions have arisen about the limits of subjecting the content to infrastructure regulations, where the dominant issue is market regulation. A new situation arises in the opposite direction when we apply the infrastructure regulation to the digital content regulation. It seems that the current reform has been created based on this kind of regulation. The issue of regulating these two areas within the scope of an audio-visual policy as an important sphere of the cultural policy has long been a subject of consideration and doubt, including in EU fora. However, the basic concept related to the issue of responsibility for activities in cyberspace is the concept of digital content. Digital content is the data that can be used to obtain information after its processing with appropriate software and hardware. An example is all the information contained in the form of electronic files, such as e-books, computer software, applications for mobile devices, and files with music, movies, and photos. Generally speaking, any good that does not exist physically but exists in the form of a digital record can become the target of cyber criminals and the subject of cyber liability for infringement of a protected good or right. Regulations regarding digital content are mainly related to the protection of consumer rights.

Yet the roles of participants in the global services market change, especially insofar as concerns electronically-provided services, and both the EU and national law will have to respond to these changes.

Final Remarks

The new information and telecommunications technologies (TIC) and the process of digitization have contributed to the emergence of new ways of accessing goods and services, while at the same time revolutionizing the traditional ways of doing business. With the development of broadband networks, not only information barriers but also territorial and language barriers have disappeared. Nowadays, a device connected to the Internet has become the basis for practically an unlimited exchange of business data. In the age of knowledge-based industries, due to the possibility of creating and accessing unlimited knowledge and information resources it has become necessary to define a new organizational and regulatory order; one which is pro-innovation. This applies, in particular, to the possibility of using educational and cultural resources of high value, supported by public funds, while maintaining the effective protection of intellectual property. This situation, together with the development of new public and private e-services, creates both new business models as well as new forms of access to culture and heritage, including the implementation of public tasks in this area. In particular, this aspect is of great importance in the current pandemic crisis, when the development of a digital-based economy, including the cultural and creative sectors, has become a priority in national and regional agendas.

In the era of digitization processes, important questions arise about the limits of subordinating content to infrastructure regulations, where the issues of dominant importance have always been issues of market-rationing and infrastructure regulation. It seems that the opposite situation now constitutes a new direction, whereby the regulation of digital content falls within the purview of the regulation of infrastructure. We can say that we are dealing with the beginning of a new approach to the issue of responsibility for digitally-shared content. The current concept of protection of digital content must be created taking into account the nature of the regulation of infrastructure. The issue of regulating these two areas in the context of a coherent policy related to the functioning of cyberspace as an important sphere of communication and exchange of goods and services has long been the subject of considerations and doubts, primarily on the part of the EU. The basic subject of exchange is digital content, i.e. data on the basis of which information can be obtained after its processing using appropriate software and hardware. Examples of such data are any information contained in the form of electronic files, such as electronic books (e-books), computer programs, applications for mobile devices, music files, movies, and photos. Generally speaking, any product that exists as a digital record may be subject to legal liability as a pro-

tected good. However, this protection is multidimensional. Regulations on digital content are mainly related to copyright and consumer protection, but it should be noted that ever more often digital content is data, often related to the person and/or activity of network users, which are not an object of consumer trade or a work within the meaning of copyright.

Recently, thanks to the global Internet network enormous changes can be observed, which have initiated extensive communication and digitization, turning what once seemed like impossible phenomena into a reality, and turning the Internet into the largest database in the world, with unlimited possibilities. In the face of all these new interrelationships in cyberspace, it is necessary to set the boundaries of legal responsibility. It is important to keep in mind that not only networks and information communication devices should be protected, but also the content of the message, i.e. digital content itself.

References

Cabrera Blázquez F.J. et al., *The European Audiovisual Industry in the Time of COVID-19*, European Audiovisual Observatory, Strasbourg 2020.

Charter on the Preservation of Digital Heritage, 15 October 2003, http://portal.unesco.org/en/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html [accessed: 18.10.2020].

Convention Establishing the World Intellectual Property Organization (WIPO), 14 July 1967, as amended on 28 September 1979, 828 UNTS 3.

Convention on Cybercrime, 23 November 2001, ETS No. 185.

Council of Europe, *Explanatory Report to the Convention on Cybercrime*, 23 November 2001, ETS No. 185.

Council of Europe, *Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime*, 13 September 1989.

Council of Europe, *Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology*, 11 September 1995.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.06.2019, p. 56.

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance), OJ L 136, 22.05.2019, p. 1.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.), OJ L 130, 17.05.2019, p. 92.

European Commission, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime"*, 26 January 2001, COM(2000) 890 final.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Towards a modern, more European copyright framework"*, 9 December 2015, COM(2015) 626 final.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "A Digital Single Market Strategy for Europe"*, 6 May 2015, COM(2015) 192 final.

European Commission, *Cybercrime*, https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en [accessed: 20.10.2020].

European Commission, *Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content*, 9 December 2015, COM(2015) 634 final – 2015/0287 (COD).

European Committee on Crime Problems, *Computer-Related Crime*, Council of Europe, Strasbourg 1990.

European Committee on Crime Problems, *Criminological Aspects of Economic Crime: Reports Presented to the Twelfth Conference of Directors of Criminological Research Institutes (1976)*, Council of Europe, Strasbourg 1977.

Hołyst B., *Kryminalistyka* [Forensic Science], 8th ed., Wydawnictwa Prawnicze PWN, Warszawa 1996.

Jakubski K.J., *Przestępczość komputerowa – podział i definicja* [Computer Crime – Classification and Definition], "Przegląd Kryminalistyki" 1997, Vol. 2.

Jenks D.A., Fuller J.R., *Global Crime and Justice*, Routledge, London–New York 2016.

Kosiński J., *Paradygmaty cyberprzestępczości* [Cybercrime Paradigms], Difin, Warszawa 2015.

Miquelon-Weismann M.F., *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, "John Marshall Journal of Computer and Information Law" 2005, Vol. 23(2).

Nowak M., *Cybernetyczne przestępstwa – definicje i przepisy prawne* [Cybercrime – Definitions and Legal Provisions], "Biuletyn EBIB" 2010, Vol. 4, http://www.ebib.pl/2010/113/a.php?nowak [accessed: 29.04.2020].

Parker D.B., *Computer Crime: Criminal Justice Resource Manual*, 2nd ed., National Institute of Justice, Washington D.C. 1989.

Pasikowska-Schnass M., *EU Support for Artists and the Cultural and Creative Sector During the Coronavirus Crisis*, May 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649414/EPRS_BRI(2020)649414_EN.pdf [accessed: 20.10.2020].

Schjolberg S., *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf [accessed: 20.10.2020].

Schneider H.J., *Kriminologie*, De Gruyter, Berlin–New York 1987.

Siwicki M., *Cyberprzestępczość* [Cybercrime], C.H. Beck, Warszawa 2013.

Sofaer A.D. et al., *A Proposal for an International Convention on Cyber Crime and Terrorism*, August 2000, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf [accessed: 15.09.2020].

Treaty on the Functioning of the European Union, consolidated version: OJ C 202, 7.06.2016, p. 47.

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych [Act of 4 February 1994 on Copyright and Related Rights], consolidated text: Dz.U. 2019 item 1231, as amended.

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny [Act of 6 June 1997. Criminal Code], consolidated text: Dz.U. 2020 item 1444, as amended.

Wallace A., Euler E., *Revisiting Access to Cultural Heritage in the Public Domain: EU and International Developments*, "IIC – International Review of Intellectual Property and Competition Law" 2020, Vol. 51.