Solutions on Blocking Access to and Removing Illegal Content on the Internet Under EU Regulations and Polish Law

FILIP RADONIEWICZ

Abstract The aim of this study is to present EU regulations aimed at tackling illegal content on the internet by blocking or removing it, as well as the state of their implementation into the Polish legal system. Accordingly, the first part describes the provisions of the Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, Directive 2017/541 of 15 March 2017 on Counteracting Terrorism, Regulation 2021/784 of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online (TERREG) and Directive 2019/790 of 17 April 2019 on Copyright and Related Rights in the Digital Single Market. The second part confronts them with Polish solutions addressing the subject of blocking and removing illegal content, as provided for in the Code of Criminal Procedure, the Act on the Internal Security Agency and on the Intelligence Agency of 24 May 2002 and the Act on Gambling Games of 19 November 2009.

Keywords: • blocking website access • terrorism • pornography • intellectual property • digital market • gambling

CORRESPONDENCE ADDRESS: Filip Radoniewicz, Ph.D., Expert, War Studies University in Warsaw, Academic Centre for Cyber Security Policy, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: filip.radoniewicz@radoniewicz.eu, ORCID: 0000-0002-7917-4059.

https://doi.org/10.4335/2022.2.13 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

European Union legislation provides that two categories of illegal content on the internet, due to its significant social noxiousness, should be tackled (i.e., blocked or removed) in an institutionalised manner, directly by state authorities. These are, of course, child pornography and so-called terrorist content.

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and replacing Council Framework Decision 2004/68/JHA (Official Journal EU L 335, 17.12.2011, p. 1) requires Member States to take measures to remove websites containing or disseminating child pornography hosted in their territory and to take steps aimed at ensuring the removal of such websites hosted outside of their territory. Under Article 2(a) any person below the age of eighteen years is a child. However, "child pornography" means (Article 2(c)):

(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;
(ii) any depiction of the sexual organs of a child for primarily sexual purposes;
(iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or
(iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes.

Furthermore, Article 25(2) of Directive 2011/93/EU allows Member States to take measures to block access to websites containing or disseminating child pornography towards on the internet within their territory, stipulating that such measures must be set following transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate to the intended purpose; the regulation is to require state authorities to inform users of the reason for any restriction. Those safeguards shall also include the possibility of judicial redress (Article 25(2)). The provisions of the Directive on safeguards refer only to measures aimed at blocking access to websites. However, in the light of Recital 47, they should refer to both the blocking and the removal of websites.

Directive 2017/541/EU of the European Parliament and of the Council of the 15th March 2017 on Combating Terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Official Journal EU L 88, 31.3.2017, p.6) contains provisions similar to those of Directive 2011/93 with regard to "online content" constituting a public provocation to commit a terrorist offence.

Pursuant to Article 3(1) and (2) of Directive 2017/541, a terrorist offence means intentional acts defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, and which meet two conditions. First, they are listed in the catalogue contained in Article 3(1) (e.g. attacks

upon a person's life which may cause death, attacks upon the physical integrity of a person, kidnapping or hostage-taking). Secondly, they were committed with one of the aims listed in Article 3(2):

(a) seriously intimidating a population;
(b) unduly compelling a government or an international organisation to perform or abstain from performing any act;
(c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

Member States are required to develop regulations to ensure the prompt removal of "terrorist content" hosted in their territory, obliging them to take measures and actions to ensure that such content hosted outside their territory is removed. It also provides, similarly to Directive 2011/93, that Member States may, when removal of the content constituting a public provocation to commit a terrorist offence at its source is not feasible, take measures to block access to such content towards internet users within their territory. Removal and blocking measures must be set following transparent procedures and provide adequate safeguards, in particular to ensure that those measures are limited to what is necessary and proportionate and that users are informed of the reason for those measures. Safeguards relating to removal or blocking shall also include the possibility of judicial redress.

The EU legislators considered the requirement for Member States to regulate the subject of making terrorist content available on the internet by means of Directive 2017/541 to be insufficient, since, even during the period of its implementation (its provisions had to be transposed into national law by 8 September 2018), work was initiated on a regulation intended to regulate only this matter.

As stated in the Explanatory Memorandum of the Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online (the so-called TERREG – from terrorism and regulation), although hosting service providers, responding to calls from public authorities, have put in place certain measures to tackle terrorist content on their services (progress has been made through voluntary frameworks and partnerships including the EU Internet Forum which was launched in December 2015 under the European Agenda on Security promoting Member States' and hosting service providers' voluntary cooperation and actions to reduce accessibility to terrorist content online), they are not sufficient. However, there is – in the Commission's view – a clear need to intensify the European Union's measures against terrorist content online. On 1 March 2018 the Commission adopted – based on Communication from the Commission of 28 September 2017 on Tackling Illegal Content Online and towards the enhanced responsibility of online platforms – a recommendation on the effective fight against illegal content online. The Commission, indicating series terrorist attacks in the EU and the fact that terrorist content is still easily accessible, found it necessary to establish a clear and harmonised legal framework for the purpose of

preventing and addressing the dissemination of terrorist content online, and that the best way to do this would be to issue a Regulation. This proposal was prepared as a contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 (Radoniewicz, 2021: 164-65).

In the light of Article 1(2) of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online (TERREG), its provisions apply to hosting service providers offering services to the society in the Union, irrespective of where their main establishment may be placed.

In the light of Article 2(1) of the Regulation, the term "hosting service provider" means a provider of Information Society services involving the storage of information provided by, and at the request of, a content provider, as well as making the information stored available to the public. This applies only to services provided to the public within the application layer. Providers of cloud infrastructure services and providers of cloud services are not considered as hosting service providers. In addition, the Regulation will not apply to electronic communications services as referred to in Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Official Journal EU L 321, 17.12.2018, p. 36), i.e. services normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, with the following types of services:

a) "internet access service" as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
b) "interpersonal communications service"; and
c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting.

"Content provider" means a user that has provided information that is, or that has been, stored and disseminated to the public by a hosting service provider.

"Terrorist content" means material belonging to at least one of the following categories, identified by their purpose, which is:

a) inciting the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such attitudes of soliciting, directly or indirectly, for instance through the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing danger that one or more such offences may be committed;
b) soliciting a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU)

2017/541, thereby causing danger that one or more such offences may be committed;

c) soliciting a person or a group of persons to participate in the activities of a terrorist group, including through delivery of information or material resources, or by financing the activities of that group in any other way within the meaning of point (b) of Article 4 of Directive (EU) 2017/541; thereby causing danger that one or more such offences may be committed;
d) providing instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;
e) posing a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, thereby causing danger that one or more such offences may be committed;

"Dissemination to the public" means the making available of information, at the request of a content provider, to a potentially unlimited number of persons. "Competent authority" shall mean a single judicial or independent administrative authority designated in a Member State for the purposes listed in Article 12(1) of the Regulation, i.e. :

a) issuing removal orders pursuant to Article 3;
b) scrutinising removal orders pursuant to Article 4;
c) overseeing the implementation of specific measures pursuant to Article 5;
d) imposing penalties pursuant to Article 18.

The Regulation provides that the competent authority of each Member State shall have the power to issue a removal order requiring hosting service providers to remove terrorist content or to disable access to terrorist content in all Member States (Article 3(1)).

Where a competent authority has not previously ordered a hosting service provider to remove content, it shall contact that hosting service provider, providing it with information on the applicable procedures and deadlines, at least twelve hours before issuing the removal order. Hosting service providers shall remove terrorist content or disable access to terrorist content as soon as possible and in any event within one hour of receipt of the removal order.

Where the hosting service provider does not have its main establishment or legal representative, that authority shall submit a copy of the removal order to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative is established.

A hosting service provider may take specific measures to protect its services against the dissemination to the public of terrorist content. (Article 5(2)).

Under Article 6(1), hosting service providers shall preserve terrorist content which has been removed or access to which has been disabled as a result of a removal order, or of specific measures pursuant to Article 3 or 5, as well as any related data removed as a consequence of the removal of such terrorist content, which are necessary for:

1) administrative or judicial review proceedings or complaint-handling under Article 10
2) the prevention, detection, investigation and prosecution of terrorist offences.

Article 18 requires Member States to establish penalties (since the general term "penalties" is used, this means that they can be of any nature: legal, administrative or civil, in this case they are both administrative and legal) applicable to infringements of the Regulation by hosting providers and to take all measures necessary to ensure that they are implemented. Member States shall ensure that a systematic or persistent failure to comply with obligations pursuant to Article 3(3) is subject to financial penalties of up to 4% of the hosting service provider's global turnover of the preceding business year.

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 (Official Journal EU L 130, 17.5.2019, p. 92) focuses on three fundamental issues:

- adapting certain exceptions (e.g. text and data mining for scientific research, making copies of any work or other protected subject matter for the purpose of preserving it as national heritage) to copyright and related rights to digital and cross-border environments;
- improving licensing practices and ensuring wider access to content;
- ensuring a well-functioning marketplace for copyright.

The Directive modifies eleven directives that regulate the subject of the protection of intellectual property under EU law, including in particular Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (Official Journal EC 2001 L 167/10) and Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights (Official Journal EU 2004 L 157/45).

It aims to facilitate the use of copyright-protected material for various purposes, mainly those related to access to knowledge, by introducing mandatory copyright limitations to promote text and data mining (understood as any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes patterns, trends and correlations), digital use of works for the purpose of illustration for teaching, and the preservation of cultural heritage. In addition, it aims to facilitate licensing to ensure wider access to content, to strengthen the protection of press publications in terms of online use, and – which was controversial already at the drafting

stage – to modify the rules of using copyright-protected content by online content sharing platforms. Within the meaning of the Directive, "online content-sharing service provider" means a provider of an information society service of which the main, or one of the main purposes, is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes.

Providers of services such as not-for-profit online encyclopedia's, not-for-profit educational and scientific repositories, open source software-developing and-sharing platforms, providers of electronic communications services as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, Official Journal EU 2018 L 321/36) (pursuant to Art. 2(4) of Directive 2018/1972, are electronic communications services which means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, with the following types of services: "internet access service"; "interpersonal communications service"; services consisting wholly or mainly in the conveyance of signals, online marketplaces, business-to-business cloud services and cloud services that allow users to upload content for their own use, are not "online content-sharing service providers" within the meaning of the Directive.

An online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users.

An online content-sharing service provider shall therefore obtain authorisation from the rightsholders referred to in Article 3(1) and (2) of Directive 2001/29/EC (i.e., authorisation for any acts of communication to the public or making available to the public), for instance by concluding a licensing agreement, in order to communicate to the public or make available to the public works or other subject matter (Article 17(1) of the Directive).

If an online content-sharing service provider has not concluded relevant licensing agreements, they may avoid liability if it proves that it:

a) made best efforts to obtain relevant authorisation from the authors (e.g., attempted to conclude a licence agreement, but for some reasons beyond their control has failed to do so),
b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightsholders have provided service providers with the relevant and necessary information (it has to block access to the content it does not hold rights to

– for this purpose it is necessary to employ persons browsing the uploading of material or the use of appropriate algorithms searching for the content it did not obtain authorisation for); and in any event,

c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightsholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future upload in accordance with point (b).

A consequence of the above-discussed regulation is the necessity to filter content uploaded in the service provider's resources. At this point, it is difficult to determine whether there is validity to concerns as to whether content filtering will worsen the conditions of information circulation and thus come into conflict with the fundamental human right of freedom of expression (Machała, 2019: 987, Markiewicz, 2021). It will undoubtedly cause the operating costs of service providers to increase due to the need to invest in suitable content filtering tools. In addition, the Directive requires that blocking should be reviewed by a humans – outcomes produced by algorithms are not sufficient, since the final decision whether the request is legitimate belongs to a human (this will undoubtedly increase the operating costs of entrepreneurs as they will need to hire staff to handle this task). (Radoniewicz, 2011: 173-183)

There are exemptions from the above regulation (Article 17(6) of the Directive). They apply to new online content-sharing service providers where the services of which have been available to the public in the EU for less than three years and which have an annual turnover below EUR 10 million. However, they are obliged to make best efforts to obtain relevant authorisation from the authors and to act expeditiously upon receiving a sufficiently substantiated notice, to disable access to the notified works or other subject matter or to remove those works or other subject matter from their websites. Nevertheless, where the average number of monthly unique visitors of websites hosted by such service providers exceeds five million, calculated on the basis of the previous calendar year, they shall also 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.

Another obligation imposed by the Directive on online content-sharing service providers is to shape the cooperation with rightsholders in such a way that it does not result in the prevention of the availability of works or other subject matter uploaded by users which do not infringe copyright and related rights, including where such works or other subject matter are covered by an exception or limitation. It should not be forgotten that it is possible to use someone's copyrighted works without infringing them, and therefore without the need to obtain a licence, under:

1) the right to quote,
2) the right to criticise or review (e.g. by creating a review of a film using extracts from it),

3) the right to parody or pastiche (e.g., creating memes).

In addition, online content-sharing service providers are required to put in place an effective and expeditious complaint and redress mechanism that is 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.

The Directive provides that 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 shall duly justify the reasons for their requests. Complaints submitted under this mechanism shall be processed without undue delay, and decisions to disable access to or remove uploaded content – as signalised hereinabove – shall be subject to human review. The Directive puts emphasis on the out-of-court settlement of possible disputes, as long as it can be ensured that they can be resolved impartially and that the decision ruled under this procedure by a court or other judicial authority can be reviewed.

The proposal for the Directive was criticised at the stage of being drafted, mainly by internet users (who feared that the uploading of their own content would be prevented), intermediary providers (who did not agree with imposing on them additional obligations in the form of data filtering) and human rights defenders (pointing out that, according to the case law of the Court of Justice, the prohibition of general monitoring provided for in Article 15 of Directive 2000/31 is aimed at protecting not only online intermediaries, but also fundamental rights, including the right to conduct business, and above all – the freedom of speech and the right to the protection of personal data – judgement of 16 February 2012 in case C-360/10). (Radoniewicz 2021: 181-183)

As far as the Polish regulations on blocking access to websites are concerned, we should first mention the procedure involving online terrorist content. Pursuant to Article 32c of the Act on the Internal Security Agency and on the Intelligence Service of 24 May 2002 (Journal of Laws of 2020, item 27, as amended; hereinafter the ISA Act) for the purpose of preventing, counteracting and detecting terrorist offences and prosecuting their perpetrators, the Regional Court in Warsaw, at the request of the Head of the ISA, filed after obtaining the written consent of the Attorney General, may order a provider of electronic services, by way of a decision, to block (no possibility to remove has been foreseen) access to specific IT data related to a terrorist event or specific communication and information services aimed at or used to cause a terrorist event, available in the communication and information system, hereinafter referred to as "access block". The request shall be accompanied by material justifying the need to use this measure.

At the same time, the legislators have provided for an accelerated procedure. Namely, in urgent cases, where any delay could result in a terrorist event. The Head of the ISA, after obtaining the written approval of the Attorney General, may order to block access, at the same time requesting the court to issue a decision in this regard. The provider of electronic

services, which is to be required to block access, shall promptly perform the actions specified in the court's decision or the request forwarded to it by the Head of the ISA.

The access block is ordered for a period not longer than thirty days. If this period proves to be too short (the reasons for the block have not ceased), the Head of the ISA may file a request, approved by the Attorney General, for a single extension of the access block for a period not longer than three months.

The afore-said requests of the Head of the ISA shall be examined by a court with a panel of one judge. The entire procedure – the actions undertaken and their content are protected by the provisions of the Act on the Protection of Classified Information. Court actions related to the examination of these requests should be performed under the conditions envisaged for the provision, storage and disclosure of classified information and with appropriate application of the provisions issued on the basis of Article 181 § 2 of the Code of Criminal Procedure (the Act of 6 June 1997 – the Code of Criminal Procedure); i.e. the Regulation of the Minister of Justice of 9 September 2017 on the Manner of Handling Interrogation Protocols and Other Documents or Subject Matter Covered by the Obligation to Maintain the Confidentiality of Classified Information or to Keep the Secret relating to the Practise of a Profession or the Performance of a Function (Journal of Laws of 2017, item 1733). The Court, the Prosecutor General and the Head of the ISA shall keep in electronic form, in compliance with the provisions on the protection of classified information, a record of decisions, written approvals, orders and requests regarding an access block. The files should be stored in the court's secret office and made available only there. Only a prosecutor and the Head of the ISA may participate in the court session.

Court decisions on the application of the block may be appealed against pursuant to generally applicable rules with the Head of the ISA and the Prosecutor General. The appeal is governed by the relevant provisions of the Code of Criminal Procedure.

Pursuant to Article 32c (11), an access block shall cease in the following events:
1) the court's refusal to authorise the Head of the ISA, within five days of filing the request pursuant to paragraph 4, to order an access block;
2) the court's refusal to agree to extend the access block;
3) expiration of the period for which the access block was imposed;

if the provider of electronic services has its registered office in the territory of the Republic of Poland The Head of the ISA notifies the minister competent for the computerisation of the imposition of an access block.

It should be pointed out that the implementation of the Directive is incomplete. The judicial review for the application of an access block has been envisaged, but there is no access to the judicial route for entities affected by such a block (see Article 21(3) *in fine* of Directive 2017/541). It should be emphasised that publishing content online falls

within the scope of the freedom of speech in its broadest sense – Article 10 of the European Convention on Human Rights and Article 11 of the CFR (Matusiak-Frącczak, 2019).

Article 15f(5) of the Act of 19 November 2009 on Gambling Games (Journal of Laws of 2020, item 2094 as amended) provides for the possibility to require telecommunications undertakings providing services related to internet access to:

1) prevent access, on a free of charge basis, to websites using the names of internet domains entered in the Register of domains used to offer gambling games in violation of the Act through their removal from the communication and information systems of telecommunications undertakings, intended to change internet domain names to IP addresses, within forty-eight hours following the entry in the Register, at the latest;
2) re-route, on a free of charge basis, connections referring to the names of internet domains entered in the Register to the website maintained by the minister competent for public finance, containing a message addressed to recipients of the internet access service, comprising, in particular, information on the location of the Register, entering a searched internet domain in this Register, a list of entities legally offering gambling games in the territory of the Republic of Poland as well as notification of potential penal and fiscal liability of a participant of games arranged in violation of the Act.
3) enable access, on a free of charge basis, to websites using the names of domains deleted from the Register, within forty-eight hours following the deletion of the name of the internet domain from the Register.

The aforementioned "Register of domains intended for offering gambling games in violation of the Act" is maintained by the Minister competent for public finance in a communication and information system enabling the automatic transmission of information to communication and information systems of telecommunications undertakings and providers of payment services. Entry into the Register is undertaken for domain names which:

a) are used for arranging gambling games, or
b) serve the advertisement or promotion of gambling

- in contravention of the law, and which are available to internet users located in the territory of the Republic of Poland (see Article 15f (1-4)).

The afore-discussed regulation is not provided for in EU law. Its admissibility was explicitly stated in the Ladbrokes judgement (CJ judgement of 3 June 2010, C-258/08, Ladbrokes Betting & Gaming Ltd and Ladbrokes International Ltd v Stichting de Nationale Sporttotalisator), in which the Court of Justice stated that blocking access to websites offering illegal gambling services is a natural consequence of the legislation in force, allowing gambling services to be offered by a monopolist to the exclusion of others.

Blocking access to gambling websites that are illegal in the territory of a Member State ensures legislative effectiveness (Lewandowicz, 2017: 14-21).

Article 218a of the Code of Criminal Procedure provides for blocking access to websites as a quasi-measure to secure evidence. In the light of § 1 of this article, offices, institutions and entities conducting telecommunication activities or providing electronic services and digital service providers are obliged to immediately secure, at the request of a court or prosecutor as contained in the decision, for a specified period of time, which shall not exceed ninety days, IT data stored in devices containing this data on a carrier or in an IT system. In the matters involving the offences specified in:

- Article 200b of the Penal Code (Act of 6 June 1997, Journal of Laws of 2021, item 2345, as amended, hereinafter: the PC) (promotion and praising of paedophilic behaviour),
- Article 202 § 3 of the PC (producing, recording, importing, storing or possessing for the purpose of distribution pornographic material with the participation of a minor or related to the presentation of violence or the use of an animal, or distributing or presenting such material),
- Article 202 § 4 of the PC (recording pornographic material with the participation of a minor),
- Article 202 § 4a of the PC (storing, possessing or gaining access to pornographic material with the participation of a minor),
- Article 202 § 4b of the PC (production, dissemination, presentation, storage or the possession of pornographic material presenting a produced or processed image of a minor participating in sexual activity),
- Article 255a of the PC (dissemination of content likely to facilitate the commission of a terrorist offence),
- Chapter 7 of the Act of 29 July 2005 on Counteracting Drug Addiction (Journal of Laws of 2020, item 2050, as amended),

a security may involve the obligation to disable access to such data.

The regulation in question applies *mutatis mutandis* to the securing of content published or provided by electronic means, with the caveat that the entity obliged to comply with a court's or prosecutor's request may also be the controller of the content.

Article 218a § 4 of the CCP provides that in the event that the publication or making available of the content referred to in § 3 constitutes a prohibited act referred to in § 1, the court or prosecutor may order the removal of such content, imposing an obligation to enforce the decision on the entities referred to in § 1 or § 3.

This measure aimed at securing evidence may not be appealed against. The Code of Criminal Procedure provides that an interlocutory appeal may be brought against a decision (order) which does not preclude the rendering of a judgement or is not a decision with respect to a precautionary measure (this refers to the preventive measures listed in

Chapter X of the Penal Code), only in cases prescribed by law (Article 459 § 2 of the CCP *in fine* in connection with § 1).

In conclusion, it is worth noting that Article 218a of the CCP owes its current shape to the Act of 20 April 2021 amending the Act – the Penal Code and certain other acts (Journal of Laws of 2021, item 1023), the purpose of which was, *inter alia*, to implement Directive 2017/541/EU on Combating Terrorism. Nevertheless, the legislators at the same time basically implemented, unknowingly or accidentally, some provisions of Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography.

As it follows from the above discussion, Poland has only partially implemented the provisions of the directives imposing an obligation to develop measures to block and remove illegal content online. The provisions of Directive 2017/541 of 15 March 2017 on Combating Terrorism have been partially implemented, which, however, for the matter of tacking illegal content is not relevant due to the adoption by the EU of the TERREG Regulation, whose provisions are, after all, directly applicable.

Nothing has been done to implement Directives 2019/790 of 17 April 2019 Copyright and Related Rights in the Digital Single Market and 2011/93/EU of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography. Although, somewhat by coincidence, Article 218a of the Code of the CCP adopts analogous solutions to the latter.

References:

Machała, W. (2019) ACTA 2 czy Nihil novi? Pierwsze refleksje na temat dyrektywy Parlamentu Europejskiego i Rady o prawie autorskim na jednolitym rynku cyfrowym, *Monitor Prawniczy*, 18.

Markiewicz, R. (2021) Rozdział 9 odpowiedzialność dostawców usług udostępniania treści online (art. 17). 9.2.Treść dyrektywy. 9.2.5.Wyłączenie odpowiedzialności DUUTO. 9.2.5.1.Zasady generalne, In: Markiewicz, R. (ed.) *Prawo autorskie na jednolitym rynku cyfrowym. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790* (Warsaw: Wydawnictwo, Wolters Kluwer Polska).

Matusiak-Frącczak, M. (2019) Rozdział 3. Polskie przepisy antyterrorystyczne a wymogi prawa Unii Europejskiej, In: Cała-Wacinkiewicz, E., Menkes, J., Nowakowska-Małusecka, J. & Staszewski, W. (eds.) *W jakiej Unii Europejskiej Polska – jaka Polska w Unii Europejskiej. Instytucjonalizacja współpracy międzynarodowej* (Warsaw: Wydawnictwo C.H. Beck), pp. 25-54.

Lewandowicz, M. (2017) Wybrane aspekty nowelizacji ustawy o grach hazardowych w świetle prawa unijnego, *Europejski Przegląd Sądowy,* 8, pp. 14-21.

Radoniewicz, F. (2021) Zwalczanie nielegalnych treści w Internecie - aspekty wybrane, In: Chałubińska-Jentkiewicz, K., Nowikowska, M. & Wąsowski, K. (eds.) *Media w erze cyfrowej. Wyzwania i zagrożenia* (Warsaw: Wydawnictwo, Wolters Kluwer Polska), pp. 155-188.