Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 327–380

https://doi.org/10.4467/27204383TER.25.036.21813

Article

Commentary on the amendment of the Act on anti-terrorist activities in relation to countering the dissemination of terrorist content on the internet

MARIUSZ CICHOMSKI

https://orcid.org/0000-0003-3707-7856

Ministry of the Interior and Administration
Republic of Poland

Abstract

The article is a commentary on the *Act of 10 June 2016 on anti-terrorist activities* in terms of the provisions introduced to this regulation by the *Act of 18 October 2024 amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency*. The purpose of the introduced provisions is to ensure the application in the Polish legal order of the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*. The author recalled previous amendments to the Act on anti-terrorist activities and discussed the basic solutions contained in Regulation 2021/784 concerning hosting providers – orders to remove terrorist content and special measures, i.e. issuing decisions on hosting providers exposed to terrorist content.

Keywords

terrorism, internet content blocking, the act on anti-terrorist activities, terrorist content, hosting provider, content provider

Introduction. Amendments to the Act on anti-terrorist activities to date

By the *Act of 18 October 2024 amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency*, the application of the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online* (hereinafter: Regulation 2021/784), was ensured in the Polish legal order, which was implemented through the amendment of the *Act of 10 June 2016 on anti-terrorist activities* (hereinafter: AT Act). By the Regulation of 18 October 2024, the *Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency* (hereinafter: the Act on the ABW and the AW) was also amended, complementing the implementation of the *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA* (hereinafter: Directive 2017/541).

This was the first such significant change to the AT Act since its enactment in 2016, i.e. after nearly nine years in force. This change consisted both in broadening the scope of the regulation's normative subject matter and extending it to new categories of addressees. The previous amendments, although their number (12) may seem relatively high were of an adjusting, correcting or streamlining nature from the perspective of the mechanisms implemented earlier, and did not introduce new legal institutions significantly changing the scope of its application.

In five cases the changes concerned the inclusion of an entity that came into being as a result of the transformation of another entity after the entry into force of the original version of the AT Act. These were: the establishment of the National Revenue Administration in place of the fragmented structures of the Ministry of Finance, in particular the Customs Service, fiscal control, tax intelligence and tax administration[1], transformation of the Government Protection Bureau into the State Protection Service[2], change of the status of the Marshal Guard into a state uniformed service with the adjustment of its tasks[3], inclusion

[1] *Act of 16 November 2016 – Provisions introducing the Act on the National Revenue Administration*. The article presents the legal status as of 23 II 2025.

[2] *Act of 8 December 2017 on the State Protection Service*.

[3] *Act of 26 January 2018 – Provisions introducing the Act on the Marshal' s Guard*.

of the General Inspector of Financial Information[4], previously omitted as a result of the changed status, or statutory assignment to the National Prosecutor the tasks hitherto belonging to the Prosecutor General[5].

The next group of amendments consists of three cases of changes related to the coherence with other emerging or changing laws, in order to maintain the legislative compatibility of references or terminological correctness. In this way, the amendments introduced by the *Act of 6 March 2018 – Entrepreneurs Law*, the *Act of 21 January 2021 on foreign service* and the *Act of 11 March 2022 on defence of the homeland* should be read.

The last group of changes consists of four amendments which, although of substantive importance, remained fragmentary in nature and were intended to streamline or correct the existing provisions from the perspective of the practice of law application. Thus, by the *Act of 12 March 2022 on assistance to Ukrainian citizens in connection with the armed conflict on the territory of the country*, Art. 13 of the AT Act, which regulates issues related to the establishment of temporary radio communication installations and the construction, reconstruction or installation of cable infrastructure and other equipment or infrastructure to the extent necessary for the launch and proper operation of such installations, was made more precise. In addition, Art. 13a was added to the AT Act, according to which the Prime Minister, taking into account the possibility of a terrorist incident or a threat to public safety and order, may, by order, restrict public access to lists, registers, databases and ICT systems containing location data of technical infrastructure.

By the *Act of 7 July 2023 on amending the Act on the protection of shipping and seaports and certain other acts* a correction regarding the scope was made to Art. 24 of the AT Act by including the Polish exclusive economic zone as an area in which anti-terrorist activities may be carried out. According to the new wording of the provision, anti-terrorist activities under the principles set out in this Act may be carried out outside the borders of the Republic of Poland, in waters within the Polish SAR (search and rescue) area of responsibility, in accordance with the *International Convention on Maritime Search and Rescue, drawn up at Hamburg on 27 April 1979* and in the Polish exclusive economic zone. Similarly, the emergency services may carry out operations to deal with the consequences of a terrorist incident and, in this

[4] *Act of 30 March 2021 amending the act on counteracting money laundering and terrorist financing and certain other acts.*

[5] *Act of 7 July 2023 amending the Civil Procedure Code, the Law on the System of Common Courts, the Criminal Procedure Code and certain other acts.*

respect, shall cooperate with each other and with the services carrying out anti-terrorist activities in the aforementioned areas. In its original version, this provision limited the area of operation to the SAR area of responsibility.

Another amendment was introduced by the *Act of 17 August 2023 amending the Act – Criminal Code and certain other acts* and it concerned, in the author's opinion, the two provisions of the AT Act that were the most controversial from a constitutional perspective. The first amendment modified Art. 9 of the Act, which provides the basis for the Head of the Internal Security Agency (hereinafter: Head of the ABW) to carry out operational control in relation to foreigners for the purpose of identifying, preventing, combating and detecting terrorist offences and prosecuting their perpetrators. This provision was expanded to include an additional premise, i.e. the offence of espionage[6]. The second change concerned Art. 26(2) – the maximum period of pre-trial detention under this law was extended to 30 days. It should be emphasised that the changes introduced assumed an increase in the possibility of practical application of the aforementioned provisions. However, their aim was not to make changes that could minimise constitutional doubts[7].

A slightly larger range of changes was made to the AT Act by the *Act of 26 July 2024 on amending certain acts to improve the activities of the Armed Forces of the Republic of Poland, the Police and the Border Guard in the event of a threat to state security*. However, these changes did not create new legal institutions. Instead, their aim was to improve the functionality of the previous solutions by introducing the possibility of communicating an opinion on the appropriateness of introducing, abolishing or changing the alert level also orally, by telephone, or by means of electronic

[6] In this context, it is worth recalling, first of all, the Judgement of the European Court of Human Rights (ECHR) in the case Pietrzak v. Poland and Bychawska-Siniarska and Others v. Poland, in which the ECHR held that there had been a violation of Art. 8 of the *Convention for the Protection of Human Rights and Fundamental Freedoms* in connection with the way the system of operational control was shaped in Poland. The ECHR noted that, with regard to operational control under the AT Act, neither the introduction of covert surveillance nor its application during the initial three-month period is subject to any control by an independent body external to the officers of the Internal Security Agency (ABW) carrying out this surveillance. See: Judgement of the European Court of Human Rights in the case Pietrzak v. Poland and Bychawska-Siniarska and Others v. Poland, https://arch-bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/orzecznictwo-europejskiego-trybunalu--praw-czlowieka/listByYear,2.html?ComplainantYear=2024 [accessed: 18 V 2025].

[7] See in more detail: M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz* (Eng. Anti-terrorist activities. Commentary), Warszawa 2018, pp. 36, 76–116, 213–214, 224–229.

communication (Art. 16 of the AT Act)[8]. An analogous solution has also been adopted for the transmission of a request to mobilise assistance to the Police from the Polish Armed Forces (Art. 22 of the AT Act). The provisions have also been aligned with the *Act of 6 April 1990 on the Police* by indicating that soldiers of branches and subdivisions of the Special Forces used to assist branches and subdivisions of the Police are entitled, to the extent necessary for the performance of their tasks, to the rights of the Police officers, and the exercise of these rights takes place on the principles and in the manner specified for Police officers (also Art. 22 of the AT Act).

The need to provide a Polish framework for the application of Regulation 2021/784

To begin with, it is worth asking whether ensuring the application of Regulation 2021/784 required amendments at the statutory level and, if so, whether this could have been done on the basis of regulations other than the AT Act. The limited framework of the study does not allow for a comprehensive commentary on the individual provisions of Regulation 2021/784, and therefore, for the purposes of this article, only a synthetic discussion of the main legal instruments introduced by this regulation to prevent the dissemination of terrorist content on the internet has been made. The commentary to the individual provisions discusses the basic regulations of Regulation 2021/784 in relation to Polish solutions, as well as the issue of the choice, on national grounds, of the authority competent to fulfil obligations under Regulation 2021/784, taking into account institutional solutions adopted in other EU states. Furthermore, the procedures for issuing and challenging orders under the aforementioned regulation are described.

As mentioned in the introduction, the Act amending the AT Act and the Act on the ABW and the AW also completed the earlier implementation of Directive 2017/541. It should be emphasised, that while the application of Regulation 2021/784 was ensured by the amendment of the AT Act, the transposition of Directive 2017/541 was ensured by the amendment of the Act on the ABW and the AW. Combining in a single legislative interference the implementation of these two pieces of EU law should

[8] This issue as a de lege ferenda postulate was pointed out in: M. Cichomski, I. Idzikowska-Ślęzak, *Alert levels – practical and legal dimensions of their use*, "Terrorism – Studies, Analyses, Prevention" no. 2, pp. 251–252. https://doi.org/10.4467/27204383TER.22.025.16345.

be assessed as an optimal solution, although the two regulations, despite the convergence of the areas they cover related to the removal and blocking of online content, have a different scope of application and do not overlap.

Regulation 2021/784 came into force on 7 June 2021 and Member States had to adapt their regulations to it within one year. This is the first comprehensive piece of direct-application legislation at EU level to regulate against the dissemination of terrorist content online. However, it was preceded by other initiatives. For instance, a framework for voluntary cooperation between Member States and hosting providers was introduced in 2015. At its meeting on 22–23 June 2017, the European Council, in response to the terrorist attacks that have taken place in EU countries and the associated propaganda spread on the internet, stated that it:

> "expects industry to [...] develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts". In its Resolution of 15 June 2017 the European Parliament called on these online platforms "to strengthen measures to combat illegal and harmful content". The call for companies to take a more proactive approach when it comes to protecting their users from terrorist content was echoed by Member State ministers at the EU Internet Forum[9].

On 28 September 2017 the European Commission (EC) adopted a Communication providing guidance on the obligations of online service providers with regard to illegal content on the internet[10]. It then issued a *Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online*, which set out specific recommendations on terrorist content in Chapter 3. The Recommendation followed the European Parliament's call to strengthen measures against illegal and harmful content on the internet, in line with the horizontal framework established by *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, and in

[9] Recital 5 of *Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online*.

[10] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms*, Brussels, 28 IX 2017, COM(2017) 555 final.

response to calls from the European Council to improve the detection and removal of content on the internet that incites terrorist acts.

The next step was the adoption of Regulation 2021/784. According to the EC it is worth to notice that: *The regulatory framework to address illegal content online was further strengthened with the entry into force of the Digital Services Act on 16 November 2022. The Digital Services Act regulates the obligations of digital services that act as intermediaries in their role of connecting consumers with content, services and goods, thereby better protecting users online and contributing to a safer online environment*[11]. Under this act, the EC has gained supervisory and enforcement powers to take action against large online platforms and search engines. Among other things, it can target information requests and investigate companies' content moderation activities, with the possibility of imposing fines.

The primary motive for issuing Regulation 2021/784 was to ensure the smooth functioning of the digital single market in an open and democratic society by countering the use of hosting services for terrorist purposes and contributing to the improvement of public security across the Union[12]. The EU also aimed to improve the functioning of the digital single market by increasing legal certainty for hosting providers and user trust in the online environment, as well as strengthening guarantees on freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society as well as media freedom and pluralism. The EU legislator has recognised that online hosting providers play a key role in the digital economy by connecting businesses and citizens and facilitating public debate as well as distribution and receipt of information, opinions and ideas, which clearly contributes to innovation, economic growth and job creation in the Union[13]. In this context, it is pointed out that it is not the hosting providers that may pose a threat in terms of spreading terrorist content, but their services that may be used by third parties for this purpose. It is noted, however, that it is the hosting providers, due to their technical

[11] *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online*, 14 II 2024, COM(2024) 64 final, p. 1.

[12] Recital 1 of the Regulation 2021/784. This issue was also addressed in: the *Government draft of the Act amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency* – explanatory memorandum, print no. 661, p. 1, https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=661 [accessed: 24 XII 2024].

[13] Recital 4 of the Regulation 2021/784.

capacity, that have particular obligations towards the public to protect their services from terrorist use and to assist in countering the dissemination of this type of content online[14]. All the more so because: *Of particular concern is the misuse of those services by terrorist groups and their supporters to disseminate terrorist content online in order to spread their message, to radicalise and recruit followers, and to facilitate and direct terrorist activity*[15].

If, however, the rules for preventing and responding to the publication of terrorist content are regulated at the level of an EU regulation, i.e. an act of law directly applicable in all Member States, the question is whether there was a possibility of measures of intervention by public authorities alternative to the enactment of a law, in view of § 1(1) point 3 of the *Regulation of the Prime Minister of 20 June 2002 on "the Principles of Legislative Techniques"* (hereinafter: Principles of legislative techniques). In this case, the answer is simple. Art. 291(1) of the *Treaty on the Functioning of the European Union* requires Member States to take all measures of national law necessary to implement legally binding Union acts. In turn, the second sentence of Art. 4(3) of the *Treaty on European Union* indicates that Member States shall take any general or specific measures appropriate to ensure fulfilment of the obligations arising out of the treaties or resulting from the acts of the EU institutions. Moreover, Regulation 2021/784 itself already obliges states to take specific actions requiring legislative interference. For example, Art. 12 obliges Member States to designate competent authorities for issuing content removal orders or specific preventive measures. On the other hand, from a national perspective, in connection with Art. 7 of the *Constitution of the Republic of Poland of 2 April 1997*, the definition of the competence of the authorities is a statutory norm, and public authorities act on the basis and within the limits of the law (legality principle). Therefore, the need for statutory solutions in this respect is not in doubt.

The second general issue concerning ensuring the application of Regulation 2021/784 in Polish law remains whether it was rightly done by adding provisions to the AT Act and whether there were other possible solutions. In the context of these considerations, it will be helpful to briefly analyse the current state of the law in the area covered by the regulation and, therefore, to fulfil the obligation referred to in

[14] Recital 5 of the Regulation 2021/784.

[15] Recital 4 sentence 3 of the Regulation 2021/784.

§ 1(1) point 2 of the aforementioned Principles of legislative techniques prior to the drafting of the legislative act.

The explanatory memorandum to the Act amending the AT Act and the Act on the ABW and the AW, indicates that the subject matter of Regulation 2021/784 is currently partly covered by national regulation, which does not fully implement Directive 2017/541 in force in this area[16]. Indeed, under its Art. 21, Member States are obliged to put in place measures that will ensure, as a matter of priority, the immediate removal of internet content inciting to commit a terrorist offence hosted on servers in their territory. Under Art. 21(1) of the Directive, states are also to take action to have such content located on servers outside their territory removed. Only if removal of such content is not possible may Member States take measures to block access to it (Art. 21(2) of the Directive). Polish legislation, on the other hand, only provides for content blocking, which, in the EC's view, is not sufficient to consider the implementation correct. There is a lack of a basic mechanism to remove such content from websites in the first place. In fact, there are provisions in the Act on the ABW and the AW, according to which the Head of the ABW, with the approval of the court, may cause a so-called blocking of the availability on the internet of certain data linked to a terrorist event. Pursuant to Art. 32c of this Act, the court may order the blocking of the availability in an ICT system of certain IT data or ICT services that are linked to a terrorist incident or that make the commission of an offence of espionage plausible. It may do so upon the written request of the Head of the ABW made with the written approval of the National Prosecutor. The blocking of the availability of ICT data shall be ordered for a period of no more than 30 days with the possibility of judicial extension for a period of no more than three months. The law also provides for a simplified procedure for urgent cases[17]. In its position, the EC states that:

> Polish law does not provide for measures to ensure the immediate removal of such online content, in particular when such content is hosted on servers within Poland. Although this may vary in some individual cases, there is no reason to believe that removal of content at source would generally be impracticable. Art. 21(2) cannot be understood as a reason for a Member State not to transpose Art. 21(1).

[16] *Government draft of the Act amending the Act...*– explanatory memorandum, p. 4.

[17] Ibid.

> Indeed, under the Directive, Member States are required to transpose both provisions, so that it is possible to remove content under Art. 21(1) as a general rule and to block access under Art. 21(2) if removal is not practicable in individual cases[18].

It should also be noted that the provisions of Directive 2017/541 have not been repealed by Regulation 2021/784, which means that the two acts are complementary and should be applied in parallel. *Regulation 2021/784 imposes obligations to remove terrorist content only on hosting providers not imposing such obligations on other providers of electronic services, including, for example, so-called caching services, which are to be understood as services consisting in the automatic and short-term storage of someone else's data on an intermediary server by creating a copy of it in order to make it available to the end user more quickly*[19].

Furthermore, Directive 2017/541, unlike Regulation 2021/784, does not link terrorist content with the public nature of its dissemination as a prerequisite for being able to issue an order to remove content or block access to it. On the basis of the Directive, it is therefore possible to seek the removal of content, e.g. in restricted internet forums.

As a result, although the indicated provision of the Act on the ABW and the AW addresses the issue of blocking content on the internet, it cannot be equated with the regulatory obligations to ensure the application of Regulation 2021/784. Accordingly, Art. 32c of the Act on the ABW and the AW has been retained, but a modification has been made according to which this provision applies in cases of publication or attempted publication of terrorist content on the internet by entities that are not hosting providers within the meaning of Regulation 2021/784.

However, since the existing regulations were in the Act on the ABW and the AW, it is worth considering whether the new regulations, coinciding thematically, should also be in this Act. In the author's opinion, a positive answer to this question raises significant doubts. Indeed, ensuring the application of Regulation 2021/784 requires the designation of a competent authority on the side of the Member State. If, in the case of Poland, it was decided that it would be the Head of the ABW, this designation could be made in the pragmatic law defining the tasks and powers of this service and its organs,

[18] *European Commission's position on 9 June 2021* (ref. no. INFR(2021)2046, C(2021)3630 final), p. 7; *Government draft of the Act amending the Act…* – explanatory memorandum, p. 15.

[19] *Government draft of the Act amending the Act…* – explanatory memorandum, p. 14.

i.e. the Act on the ABW and the AW. However, the range of matters delegated by the EU legislator to be regulated at national level is much broader. Indeed, Regulation 2021/784 defines not only the sphere of action of the competent authorities, but also the rights, including the right to challenge decisions of state authorities, and the obligations of hosting providers and content providers, as well as the system and level of penalties that may be imposed on them. This is therefore well beyond the sphere that can be normalised in a pragmatic law for a particular formation. Pragmatic laws should not, although this currently happens, regulate the rights and obligations of others. Furthermore, in the author's view, the current positioning of the provisions of Art. 32c of the Act on the ABW and the AW should be regarded as legislatively questionable. These provisions were introduced by amending provisions as part of the original text of the AT Act in 2016, so the legislature could already have included them in the act. Another decision was probably dictated by the fact that the construction of the provisions in the procedural dimension is similar to the legal institution of operational control regulated in Art. 27 of the Act on the ABW and the AW (analogous to the pragmatic laws of other services authorised to conduct it, e.g. in Art. 19 of the Act on the Police). Thus, it is not the provisions ensuring the application of Regulation 2021/784 that should be included in the Act on the ABW and the AW, but conversely, it is the existing provisions related to the blocking of content included in this act that could ultimately be included in the AT Act. As an aside, it is worth noting, that this observation also applies to Art. 32a–32b of the Act on the ABW and the AW concerning the conduct of security assessments of ICT systems of public administration bodies and critical infrastructure operators, as well as warning systems by the Internal Security Agency (ABW).

Another argument confirming the correctness of the approach to the provisions related to Regulation 2021/784 is provided by § 2 of the Principles of legislative techniques, pursuant to which the act should comprehensively regulate a given area of matters and not leave important fragments of this area outside the scope of its regulation. In the context related to the issue of threats of a terrorist nature, the basic regulation is the AT Act and it is the act which, as a rule, should contain the matters related to this issue. This argument is pertinent also with regard to the second potential alternative location of the provisions for the application of Regulation 2021/784, i.e. to regulate this issue in a new separate regulation.

As an aside, it is worth noting that, for analogous reasons, the provisions of the current *Act of 13 April 2016 on the security of trading in explosives*

precursors, which serves to apply *Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors,* could be incorporated into the AT Act. The Regulation was issued in the wake of the attacks by Norwegian extremist Anders Breivik on the Norwegian Prime Minister's residence and on participants in the Norwegian Labour Party's youth camp[20].

Basic solutions included in Regulation 2021/784 in relation to countering the dissemination of terrorist content on the internet – removal orders and specific measures

In the context of the commentary to the individual provisions of the AT Act, numerous references to the provisions and recitals of Regulation 2021/784 are necessary, but they serve to interpret the individual provisions of Polish law. However, a synthetic presentation of the basic instruments for preventing the dissemination of terrorist content on the internet introduced by Regulation 2021/784 is necessary. Enabling their application in Poland is the goal of activities at the level of the national legislator.

For the purposes of this study, two basic mechanisms can be distinguished for countering the dissemination of mentioned content on the internet:

- issuing orders requiring hosting providers to remove terrorist content or prevent access to terrorist content in all Member States, in accordance with Art. 3 of Regulation 2021/784 (hereinafter: removal orders);
- issuing decisions on hosting providers exposed to terrorist content, based on Art. 5 of Regulation 2021/784 (hereinafter: specific measures).

These two mentioned instruments are matched by a number of additional powers and procedural rules, as well as mechanisms and

[20] See in more detail: M. Cichomski, P. Marchliński, *Krajowe rozwiązania w zakresie bezpieczeństwa obrotu prekursorami materiałów wybuchowych – po zamachu terrorystycznym w Norwegii 22 lipca 2011 r. w kontekście nowych zadań Policji* (Eng. National security arrangements in the trade in explosives precursors – after the terrorist attack in Norway on 22 July 2011 in the context of new police tasks), in: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (eds.), Szczytno 2016, pp. 591–600.

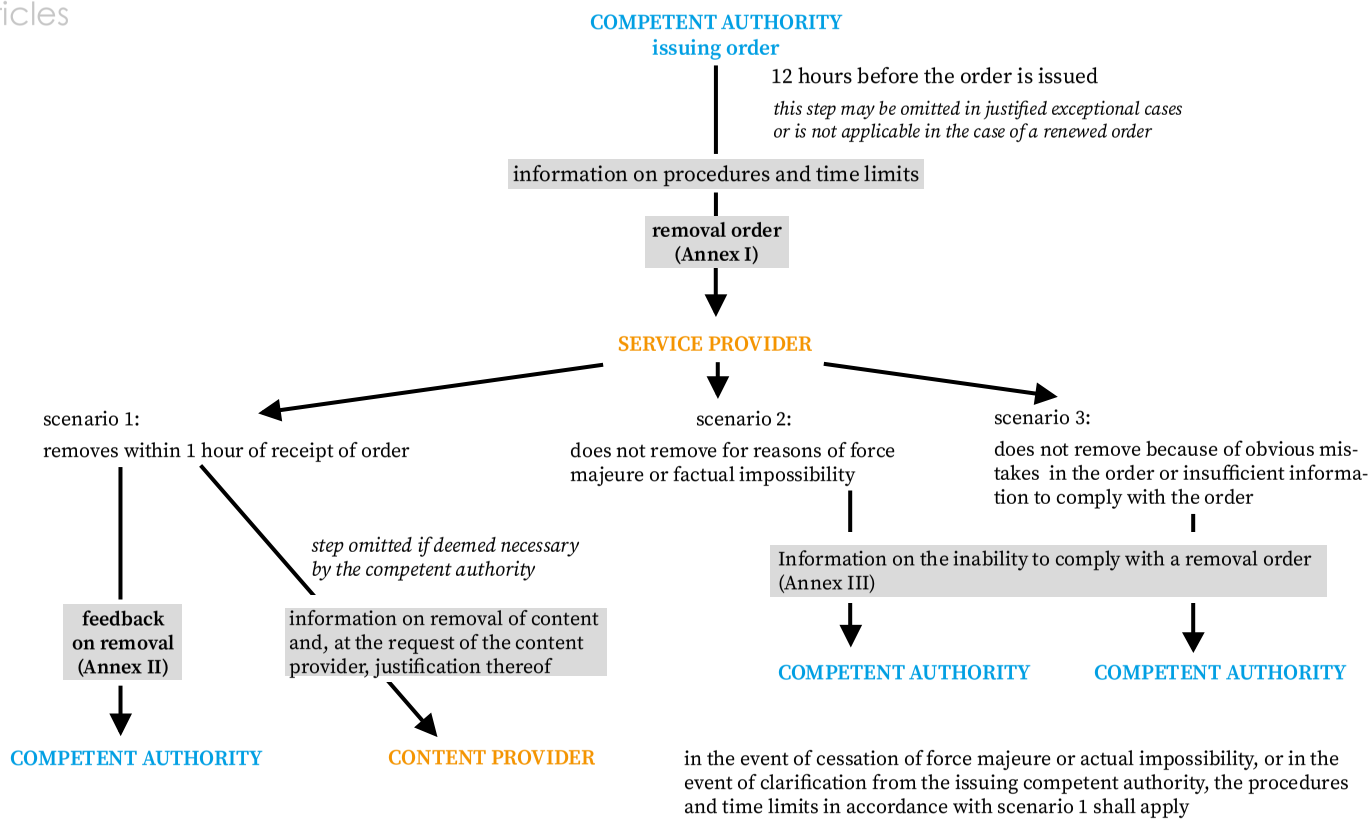
tools for cooperation between EU states, the EC and the European Union Agency for Law Enforcement Cooperation, or Europol, as well as hosting providers (schemes 1 and 2).

The first of the instruments mentioned above – the removal order – implies that the competent authority of each Member State has the power to issue a removal order obliging hosting providers to remove terrorist content or to prevent access to terrorist content in all Member States. Following the order, the hosting providers shall remove or disable access to the content in all Member States as soon as possible, no later than one hour after receipt of the removal order.

The orders are issued on a standardised form and contain such information as: the identification of the competent authority issuing the order, the grounds for the order, the exact standardised format for addressing the resource (URL address) and, if necessary, additional information to identify terrorist content or information on the legal remedies available to the hosting provider and the content provider. The hosting providers shall then inform the competent authority of the execution of the order – indicating in particular the time of removal or disabling access to the content (a model removal order is set out in Annex I to Regulation 2021/784).

If such an order is being issued for the first time in respect of a particular hosting provider, it shall be preceded by the provision of information to that provider on the applicable procedures and time limits at least 12 hours prior to the issuing of the removal order. This obligation may be omitted in particularly justified cases.

If the hosting provider is unable to comply with the order due to force majeure or actual impossibility attributable to it, including technical or operational reasons which can be objectively justified, the hosting provider shall inform the competent authority which issued the order and the one-hour time limit for removing the content or blocking access to it shall start to run as soon as the aforementioned reasons cease to exist. If, on the other hand, the hosting provider is unable to comply with the order because it contains errors or does not contain sufficient information to comply with it, the hosting provider shall inform the competent authority which issued the removal order. In this case, the time limit starts to run as soon as the hosting provider has received the necessary clarifications. The order shall become final either after the expiry of the time limit for lodging an appeal, where it was not lodged in accordance with national law, or as a result of the maintenance of the removal order following an appeal.



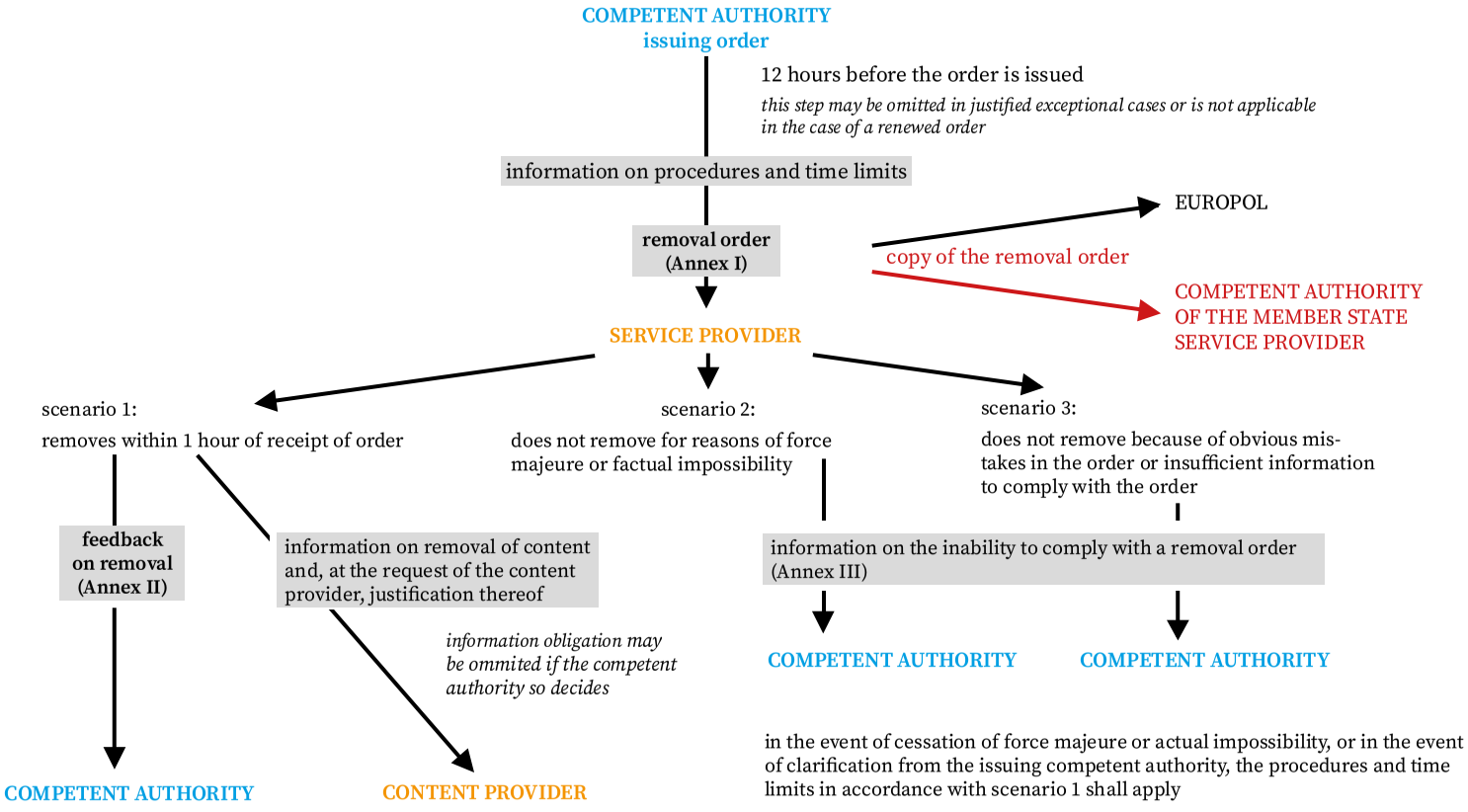
Scheme 1. Procedure for the imposition of a removal order of terrorist content where the main organisational unit or legal representative of the hosting provider is located in the same Member State as the competent authority issuing the order.

Source: study by Aneta Suda, *Mechanisms for blocking terrorist content on the internet in the light 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*, presentation by the Ministry of Internal Affairs and Administration prepared for the Interministerial Team for Terrorist Threats.

Mention should be made of the mechanism for verifying removal orders issued by the competent authorities of other Member States and identifying possible infringements in this respect (Art. 4 of Regulation 2021/784). This is the so-called cross-border removal procedure (scheme 3). According to this solution, in the event that the hosting provider does not have a main establishment or a legal representative in the Member State of the competent authority that issued the order, this authority shall transmit a copy of the removal order to the competent authority of the Member State in which the hosting provider has its main establishment or in which its legal representative is resident or established.

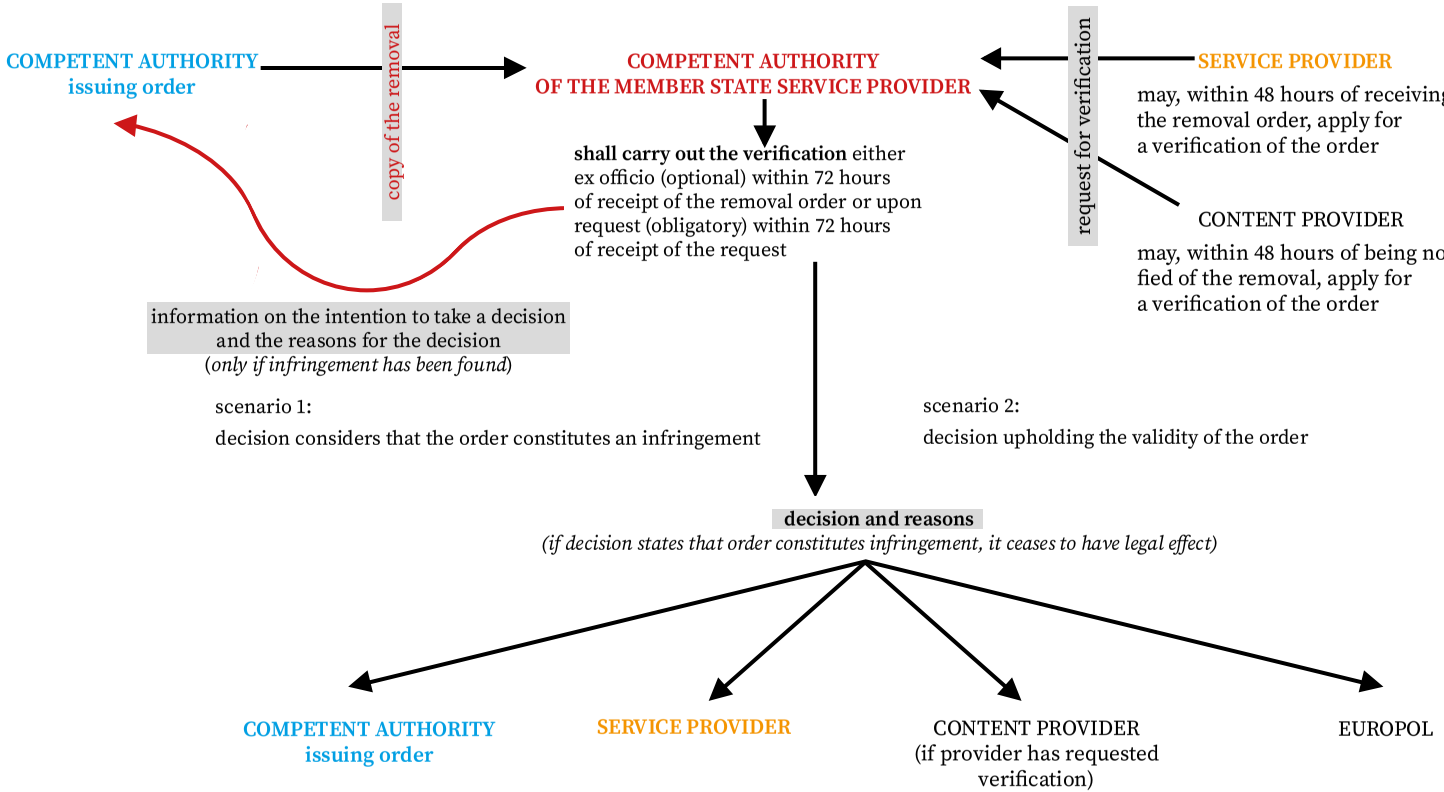
The competent authority of the Member State in which the hosting provider has its main establishment or in which its legal representative is resident or established may, on its own initiative, within 72 hours of receipt of a copy of that order, review it in order to establish that it does not seriously or manifestly infringe the legal grounds for issuing it or fundamental rights and freedoms. If such an infringement is found, it shall take a reasoned decision on the matter within the same time limit.

Hosting providers and content providers also have the possibility to initiate a verification action – within 48 hours of receiving the order, they can request a verification to the competent authority of the Member State where the hosting provider has its main establishment or where its legal representative is resident or established. This verification shall be carried out within 72 hours of receipt of the request. As a result, the competent authority shall take a decision, the issuing of which shall be preceded by communication to the issuing authority of its intention to do so. When a decision is taken, it shall immediately notify the competent authority which issued the removal order, the hosting provider, the content provider which requested the review and Europol of the decision. Where it is determined that a removal order constitutes an infringement, it shall cease to have legal effect and the hosting provider shall immediately restore the content in question or access to it.



Scheme 2. Procedure for the imposition of an order for the removal of terrorist content where the main organisational unit or legal representative of the hosting provider is not located in the same Member State as the competent authority issuing the order.

Source: Study by Aneta Suda, *Mechanisms for blocking terrorist content on the internet in the light 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*, presentation by the Ministry of Internal Affairs and Administration prepared for the Interministerial Team for Terrorist Threats.



Scheme 3. Procedure for the imposition of a cross-border removal order.

Source: Study by Aneta Suda, *Mechanisms for blocking terrorist content on the internet in the light 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*, presentation by the Ministry of Internal Affairs and Administration prepared for the Interministerial Team for Terrorist Threats.

The second main mechanism identified for preventing and responding to the dissemination of terrorist content on the internet (specific measures) is the issuing of decisions on hosting providers exposed to terrorist content and the supervision of their implementation of specific measures.

Explaining the *ratio legis* of this solution, the EU legislator pointed out that:

> With a view to reducing the accessibility of terrorist content on their services, hosting service providers exposed to terrorist content should put in place specific measures taking into account the risks and level of exposure to terrorist content as well as the effects on the rights of third parties and the public interest to information. Hosting service providers should determine what appropriate, effective and proportionate specific measure should be put in place to identify and remove terrorist content. Specific measures could include appropriate technical or operational measures or capacities such as staffing or technical means to identify and expeditiously remove or disable access to terrorist content, mechanisms for users to report or flag alleged terrorist content, or any other measures the hosting service provider considers appropriate and effective to address the availability of terrorist content on its services[21].

A hosting provider recognised as a provider exposed to terrorist content shall include in its contractual terms as well as apply provisions to counter the use of its services for the public dissemination of terrorist content and shall take specific measures to this end. These may include, for example:

- technical and operational means or capabilities, such as appropriate personnel or technical means for the purpose of identifying and promptly removing or preventing access to terrorist content;
- easily accessible and user-friendly mechanisms for users to report or flag alleged terrorist content to the hosting provider;
- other mechanisms to raise the awareness of the availability of terrorist content on its services, such as mechanisms to moderate users;
- other measures that the hosting provider considers appropriate to counter the availability of terrorist content on its services.

[21] Recital 22 of the Regulation 2021/784.

The premise is that the specific measures are intended to effectively reduce the level of exposure of the hosting provider's services to terrorist content, to be targeted and proportionate, and to be applied in a careful and non-discriminatory manner, taking into account full respect for the rights and legitimate interests of users.

A hosting provider should be deemed to be exposed to terrorist content where the competent authority of the Member State in which the hosting provider has its main establishment or in which its legal representative is resident or established has decided that the provider is exposed to terrorist content. This decision should be taken on the basis of objective factors, such as the receipt by the provider of at least two final removal orders of such content in the last 12 months.

Upon receipt of the decision, the hosting provider shall, within three months, notify the competent authority of the specific measures it has taken or intends to take to ensure compliance with its obligations. Thereafter, once a year, the hosting provider shall draw up a report on their implementation.

If the competent authority considers that the specific measures taken do not comply with the requirements, it shall address a decision to the hosting provider requiring it to take the necessary measures. The hosting provider may choose which type of specific measures it will take. It may also, at any time, request the competent authority to review and, where appropriate, amend or revoke its decision to designate it as a hosting provider exposed to terrorist content.

To conclude this part of the article, it is worth recalling some statistics on the application of Regulation 2021/784 until 31 December 2023[22]. According to the EC's findings, Member States have issued 349 removal orders of terrorist content. This option was used by the competent authorities of six Member States, i.e. Spain – 62 orders, Romania – 2 orders, France – 26 orders, Germany – 249 orders (all issued after the attack carried out by Hamas on 7 October 2023), Czech Republic – 2 orders, Austria – 8 orders. The orders were addressed to the following entities, among others: Telegram, Meta, JustPaste.it, TikTok, DATA ROOM S.R.L., FlokiNET S.R.L., Archive.org, SoundCloud, X, Jumpshare, KrakenFiles.com, Top4toP and Catbox.

[22] Based on the *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784*...

Out of 349 removal orders issued, only in 10 cases did the hosting provider fail to remove the terrorist content or block it within the maximum deadline, i.e. within one hour of receiving the order. In only one case did the hosting provider state that it was impossible to comply with the order.

No order was subject to the review in the cross-border removal order procedure. Consequently, there was no case recorded stating that the issued order made such a violation.

To date, no hosting provider has been identified as being exposed to terrorist content and therefore no provider has been required to implement special measures.

Noteworthy, no order issued has been challenged in court to date.

Commentary on specific provisions of the AT Act in relation to the prevention of the dissemination of terrorist content on the internet

Two groups of provisions were introduced into the AT Act by the Act amending the AT Act and the Act on the ABW and the AW. The first is the expansion of the statutory vocabulary contained in Art. 2 of the amended Act to include three definitions, each of which includes a reference to Regulation 2021/784. The second group of provisions is covered by a new unit of statutory systematisation labelled as Chapter 5a – countering the dissemination of terrorist content on the internet. It contains six provisions related to the designation of the competent authority on the national side, procedural provisions and provisions specifying administrative penalties, i.e. legal norms directly ensuring the application of Regulation 2021/784. Moreover, the title of the Act was supplemented with a reference to this regulation.

The next part of the article is a commentary on the individual provisions.

Art. 1. The Act of 10 June 2016 on anti-terrorist activities (Journal of Laws of 2024, item 92 and 1248) is amended as follows:

1) The following reference is added to the title of the Act:

"1) This Act serves to apply the Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Official Journal of the EU L 172 of 17.05.2021, p. 79)".

By supplementing the title of the AT Act with a reference to the application of Regulation 2021/784, the obligation under § 19a(2) of the Principles of legislative techniques was fulfilled. According to it, in the case of a law the enactment of which is linked to the issuance or validity of a directly applicable normative act established by an EU institution, the specification of the subject matter of the law shall be followed by a reference to the title of the law indicating the normative act with which the law is linked, which is expressed in particular by the phrase, "this law serves to apply... [title of the act]".

2) In Art. 2 point 7, the full stop shall be replaced by a semicolon and the following points 8–10 shall be added:
[whenever the Act refers to:]
"8) hosting service provider – means a service provider of services consisting in storing information provided by and at the request of a content provider, as referred to in Art. 2(1) of the Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Official Journal of the EU L 172 of 17.05.2021, p. 79), hereinafter referred to as "Regulation 2021/784"; (…)

According to Art. 2 point 1 of Regulation 2021/784 'hosting service provider' means a provider of services (as defined in letter (b) of Art. 1 of *Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services)*, storing information provided by and at the request of a content provider. According to the Directive, 'service' means any information society service, that is to say any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. Except that 'at a distance' means that the service is provided without the simultaneous presence of the parties. 'By electronic means' means that the service is sent and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and which is entirely transmitted, conveyed and received by wire, radio waves, optical or other electromagnetic means. 'At the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

It is worth noting recital 13 of the cited regulation, according to which:

> In order to effectively address the dissemination of terrorist content online, while ensuring respect for the private life of individuals, this Regulation should apply to providers of information society services which store and disseminate to the public information and material provided by a user of the service on request, irrespective of whether the storing and dissemination to the public of such information and material is of a mere technical, automatic and passive nature. The concept of 'storage' should be understood as holding data in the memory of a physical or virtual server. Providers of 'mere conduit' or 'caching' services, as well as of other services provided in other layers of the internet infrastructure, which do not involve storage, such as registries and registrars, as well as providers of DNS (domain name systems), payment or DDoS (distributed 'denial of service' attack) protection services, should therefore fall outside the scope of this Regulation.

Regulation 2021/784 extended its scope to hosting providers offering services in the EU, i.e. enabling natural or legal persons, in one or more Member States, to use services of a hosting provider who has a substantial link with the Member State, either by virtue of having an establishment in the Union or by virtue of specific factual criteria, such as having a significant number of users of its services in one or more Member States or directing its activities towards one or more Member States (Art. 2 points 4 and 5 of the Regulation). This offering of services must be carried out to the extent that the hosting providers disseminate information to the public (Art. 1(2) of the Regulation), regardless of the location of their main organisational unit, i.e. their head office or registered office, where the main financial functions are performed and operational control is exercised (Art. 2 point 9 of the Regulation). However, it should be borne in mind that where access to information requires registration or admission to a group of users – under Art. 2 point 3 and Recital 14 of the Regulation – this information should only be considered publicly disseminated if users seeking access to the information are automatically registered or admitted to a group of users, without the need for a human decision as to whom to grant such access.

In order to ensure a workable application of the Regulation with regard to hosting providers, an obligation has been introduced under Art. 17 of Regulation 2021/784 whereby, if the provider does not have a main establishment in the EU, the provider shall designate in writing

a natural or legal person as its legal representative in the Union for the purpose of receiving, complying with and implementing removal orders and decisions issued by the competent authorities. Furthermore, the provider shall delegate to its legal representative the necessary powers and resources to comply with those removal orders and decisions and to cooperate with the competent authorities. The hosting provider shall notify the appointment of the legal representative to the competent authority of the Member State in which its legal representative is resident or established and shall make information on the legal representative publicly available. The legal representative may be held liable for infringements of this Regulation, without prejudice to the hosting provider's liability and legal action against the hosting provider.

In the author's opinion, the aforementioned issue is of key importance to the efficiency of application of Regulation 2021/784 itself from the perspective of the effectiveness of removal or blocking of terrorist content. Indeed, in contrast to solutions adopted at the level of individual states, including the mechanisms in force in Poland set out in the Act on the ABW and AW, it can be effectively applied to content posted at a hosting provider located outside a given state. An analogous opinion was expressed by the EC:

> While voluntary measures and non-binding recommendations contributed to reduce the availability of terrorist content online, limitations including the small number of hosting service providers adopting voluntary mechanisms[23] as well as the fragmentation of procedural rules across Member States limited the effectiveness and the efficiency of cooperation among Member States and hosting service providers and made it necessary to establish regulatory measures[24]. Therefore, the effective application of the Regulation is key to address the dissemination of terrorist content online. The Commission has proactively supported national competent authorities in this process[25].

[23] *Commission Staff Working Document Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online*, Brussels, 12 IX 2018, SWD(2018) 408 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN [accessed: 4 V 2023].

[24] Ibid.

[25] *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784...*, p. 4.

9) in Art. 2 in point 7, the full stop shall be replaced by a semicolon and the following points 8–10 shall be added: […]
[whenever the Act refers to:]
"9) content provider – it shall mean the user referred to in Art. 2 point 2 of the Regulation 2021/784;"

According to Art. 2 point 2 of Regulation 2021/784 a 'content provider' means a user that has provided information that is, or that has been, stored and publicly disseminated by a hosting provider; In turn 'public dissemination' means the making available of information, at the request of a content provider, to a potentially unlimited number of persons (Art. 2 point 3 of Regulation 2021/784).

While the EU legislator clearly emphasises the socially and economically crucial role of hosting providers as connectors between businesses and citizens establishing a space for public debate or exchange of information, and whose activities can be used by third parties to transmit terrorist content, it is explicitly indicated with regard to the content provider that it bears editorial responsibility for its activities.

2) in Art. 2 in point 7, the full stop shall be replaced by a semicolon and the following points 8–10 shall be added: […]
[whenever the Act refers to:]
10) terrorist content – means the materials referred to in the Art. 2 point 7 of the Regulation 2021/784.

According to Art. 2 point 7 of Regulation 2021/784 terrorist content means material that:

- incites the commission of one of the offences referred to in Art. 3(1) letters (a)–(i) of Directive (EU) 2017/541 (indicated below), where such material, directly or indirectly, for instance, by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;
- induces a person or a group of persons to commit or to contribute to the commission of one of the following offences within the meaning of Directive 2017/541;
- solicits a person or a group of persons to participate in the activities of a terrorist group;

– provides 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 following offences within the meaning of Directive 2017/541;
– constitutes a threat of committing one of the following offences within the meaning of Directive 2017/541.

According to Art. 3(1) letters (a)–(j) of Directive 2017/541, terrorist offences are intentional acts, defined under Polish law as offences which, by their nature or context, are capable of causing serious damage to a State or an international organisation and have been committed with a specific purpose. They are:

a) attacks upon a person's life which may cause death;
b) attacks upon the physical integrity of a person;
c) kidnapping or hostage taking;
d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
e) seizure of aircraft, ship or other means of public or goods transport;
f) manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of such weapons;
g) release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life;
h) interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;
i) illegal interference with systems, as referred to in Art. 4 of Directive of the European Parliament and of the Council 2013/40/EU (1), where Art. 9(3) or Art. 9(4) letter (b) or (c) of this Directive applies, and unlawful interference with data, as referred to in Art. 5 of that Directive, in cases where Art. 9(4) letter (c) of that Directive applies[26];

[26] According to Art. 4 and 5 of the *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council*

j) threatening to commit any of the acts listed.

According to Art. 3(2) of Directive 2017/541, the indicated categories of offences are terrorist offences if committed with the aim of:

- serious intimidation the population;
- unlawful compelling a government or an international organisation to take or refrain from taking some action;
- serious destabilisation or destruction of the fundamental political, constitutional, economic or social structures of the state or international organisation concerned.

The cited definition, in principle, corresponds to the definition of a terrorist offence in Art. 115 § 20 of the *Act of 6 June 1997 Criminal Code*, according to which a terrorist offence is a criminal act punishable by imprisonment of at least 5 years, committed with the aim of:

1) seriously intimidating a number of persons,
2) forcing a public authority of the Republic of Poland or of another state or an authority of an international organisation to take or to refrain from taking a specific action,
3) causing serious disturbances in the system or economy of the Republic of Poland, another state or an international organisation,

- as well as a threat to commit such an act.

However, the Polish definition, contrary to the definition in Directive 2017/541, does not specify the types of underlying offences, but only defines them by indicating that their upper limit is at least 5 years. As an aside, it is worth noting that this dissimilarity has been pointed out as a lack of proper implementation of the Directive[27], but on the other hand it provides flexibility in the application of the national regulation.

In the context of the application of Regulation 2021/784 and the safeguarding against possible abuse, it is most important that the disclosure of terrorist content is properly assessed. Recital 11

Framework Decision 2005/222/JHA, unlawful interference with information systems consists of inputting computer data, transmitting, damaging, deleting, deteriorating, altering or suppressing such data or rendering such data inaccessible. Unlawful data interference, on the other hand, is the intentional and unlawful deleting, damaging, deteriorating, altering or suppressing computer data on an information system or rendering such data inaccessible.

[27] This issue was raised, inter alia, during a visit to Poland by the United Nations Counter-Terrorism Committee Executive Directorate (UN CTED), to evaluate Poland's implementation of UN Security Council resolutions on counter-terrorism.

of that Regulation provides guidance in this regard. According to it, in view of the need to counter the most harmful terrorist propaganda on the internet, the definition of terrorist content should include:

> (...) material that incites or solicits someone to commit, or to contribute to the commission of, terrorist offences, solicits someone to participate in activities of a terrorist group, or glorifies terrorist activities including by disseminating material depicting a terrorist attack. The definition should also include material that provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, as well as chemical, biological, radiological and nuclear (CBRN) substances, or on other specific methods or techniques, including the selection of targets, for the purpose of committing or contributing to the commission of terrorist offences. Such material includes text, images, sound recordings and videos, as well as live transmissions of terrorist offences, that cause a danger of further such offences being committed.

The remainder of this recital of Regulation 2021/784 indicates that, in assessing whether material constitutes terrorist content, competent authorities and hosting providers should take into account factors such as the nature and content of the communications, the context in which the communications are presented and the extent to which the communications are likely to result in effects detrimental to the safety and security of persons. However, an important limitation is formulated in this recital. According to it, an important factor in this assessment is that the material in question has been produced by a person, group or entity on the EU list of persons, groups and entities involved in terrorist acts and subject to restrictive measures, that it is attributable to such a person, group or entity, or that it is disseminated on behalf of such a person, group or entity. On the one hand, this is intended to ensure freedom of speech and opinion, but on the other hand, when interpreted literally and not purposefully, it constitutes narrowing the content in question to a link to persons, groups or entities on the EU list of persons, groups and entities involved in terrorist acts. Indeed, not every provider of such content can explicitly demonstrate such a link.

By contrast, Art. 1(3) of Regulation 2021/784 explicitly indicates that material publicly disseminated for educational, journalistic, artistic or research purposes, or for the prevention or combating of terrorism, including material intended to express polemical or controversial views in

the context of a public debate, shall not be deemed to be terrorist content. Moreover, it is to be determined by means of an assessment what the actual purpose of the dissemination of the content in question is. It is worth mentioning in this context Recital 12 of Regulation 2021/784. According to it, in determining whether material provided by a content provider constitutes 'terrorist content', particular consideration should be given to the right to freedom of expression and information, including freedom and pluralism of the media, and freedom of the arts and sciences.

From a legislative perspective, it is worth noting the structural consistency of the terminology used in the Criminal Code, the AT Act and Regulation 2021/784. The indicated legal acts use the terms 'terrorist offence', 'terrorist event' and 'terrorist content' respectively. However, not all Polish legal acts include them. For example, the Act on the ABW and the AW refers to the 'crime of terrorism'.

> Art. 26a. The Head of the ABW is the competent authority within the meaning of Regulation 2021/784.

In analysing the scope of the indicated jurisdiction, attention should be drawn at the outset to the previously mentioned Art. 12 of Regulation 2021/784, according to which each Member State shall designate the authority or authorities competent to:

- issue orders requiring hosting providers to remove terrorist content or prevent access to terrorist content in all Member States (removal order),
- verify removal orders issued by the competent authorities of other Member States and to identify possible infringements in this respect (procedure for cross-border removal orders),
- supervise the implementation of specific measures by the hosting provider,
- impose penalties for breaching the provisions of the regulation in question.

The above indication does not exhaust all the obligations and powers imposed on the competent authorities by other provisions of Regulation 2021/784. In this respect, it is possible to point out, inter alia, the following:

- extending the period of retention of terrorist content that has been removed or to which access has been prevented, as a result of a removal order (Art. 6(2) of Regulation 2021/784),

- issuing decisions on hosting providers exposed to terrorist content and to supervise their implementation of specific measures, based on Art. 5 of Regulation 2021/784,
- carrying out cooperation, including the exchange of information, with other competent authorities established by the other Member States, Europol and hosting providers, in accordance with Art. 14 of Regulation 2021/784,
- publication of the report, pursuant to Art. 8 of Regulation 2021/784,
- transmission of annual information to the EC on the basis of Art. 21 of Regulation 2021/784.

In the aforementioned Art. 12 of Regulation 2021/784, the EU legislator provided for the possibility of designating various authorities as the competent authorities for the exercise of the indicated powers and duties. The Polish legislator did not use this possibility and designated the Head of the ABW as the only authority competent on national grounds. This solution seems to be optimal and is in line with the entirety of the national norms in this respect, in connection with which at least four aspects should be noted. Firstly, the Head of the ABW under Art. 3(1) of the AT Act is responsible for the prevention of terrorist incidents[28]. Secondly, on the basis of Art. 5(1) point 1 of the Act on the ABW and the AW, the tasks of this formation include, inter alia, the identification, detection and prevention of terrorist offences, and terrorist content is largely used to carry out terrorist attacks. Thirdly, the Head of the ABW had already been given the authority to block terrorist content under the provisions of the Act on the ABW and the AW. Fourthly, the ABW also has an organisational structure in the form of the Counter-Terrorism Centre of the Internal Security Agency, fully equipped for this purpose, operating on a 24/7 basis.

According to Recital 35 of Regulation 2021/784, Member States should be able to decide on the number of competent authorities to be designated and whether they should be administrative, law enforcement or judicial authorities. These authorities must carry out their tasks in an objective and non-discriminatory manner and should not seek instructions from any other authority in relation to the performance of the tasks assigned to them under this Regulation. Importantly, however, this should not preclude the exercise of supervision in accordance with national constitutional law.

[28] See in more detail: P. Burczaniuk, *Tasks and powers of criminal law enforcement authorities in combating terrorism in Poland – a legal perspective*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 2, pp. 9–30. https://doi.org/10.4467/27204383TER.22.024.16344.

Pursuant to Art. 12(4) of Regulation 2021/784, the EC has set up and keeps up to date an online register containing a list of the competent authorities in each country and their contact points designated or established pursuant to Art. 12(2) of the Regulation, referred to later in the commentary to Art. 26b of the AT Act[29]. According to the register published on the EC website, on the day the Polish Parliament adopted content blocking solutions, 25 out of 27 EU Member States provided such information (notifications were not made by Slovenia and Portugal)[30]. Out of this group, 13 countries designated the competent authority – similarly to Poland – from among services of a police or specialised character, four countries indicated the competence of an organisational unit functioning within the Ministry of Interior and the same number of countries in other central offices, e.g. in the case of Hungary – the National Media and Infocommunications (Nemzeti Média- és Hírközlési Hatóság), in Austria it is the Communications Authority (Kommunikationsbehörde Austria). In two countries it is the prosecuting authority and in one the court has jurisdiction[31].

The decision of the Polish legislator, i.e. to designate the Head of ABW as the competent authority, is in line with EU guidelines and does not deviate from the solutions adopted in other countries, but the practice in this respect differs.

> Art. 26b. 1. The Head of the ABW shall designate a contact point within the ABW as referred to in Art. 12(2) of Regulation 2021/784, operating on a 24/7 basis.
> 2. Information on the seat and contact details of the contact point referred to in paragraph 1, as well as on how to submit requests for clarification and feedback on removal orders obliging hosting providers to remove terrorist content or prevent access to terrorist content, hereinafter referred to as 'removal orders', shall be made available in the Bulletin of Public Information on the webpage of the ABW.

[29] *List of national competent authority (authorities) and contact points,* European Commission, 27 I 2025, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en?prefLang=pl [accessed: 15 II 2025].

[30] As of 23 II 2025, the only country that had not made a notification was Portugal.

[31] See in more details: *Government draft of the Act amending the Act…*

Art. 12(2) of Regulation 2021/784 requires Member States to ensure that a contact point is designated or established within the authority competent for issuing removal orders to deal with requests for clarification and feedback on such orders. In Poland, the consequence of the choice of the Head of the ABW as the competent authority was that he designated a contact point within the Agency he heads. Member States were also obliged to ensure that information on the contact point was publicly available.

It is worth noting that the Polish legislator has extended the minimum scope of information to be included on the webpage in line with the requirements under Regulation 2021/784. In addition to information on the contact point, the webpage must also contain information on how to submit requests for clarification and feedback on removal orders. According to the notice on the webpage of the ABW:

> Requests for clarification on removal orders obliging hosting providers to remove terrorist content or to prevent access to terrorist content, submitted using the model set out in Annex III to Regulation 2021/784, may be addressed in hard copy to the postal address of the contact point or in electronic form to the e-mail address of the contact point. Feedback after the removal or disabling of access to terrorist content, submitted using the model set out in Annex II to Regulation 2021/784, will be provided in the same form[32].

It should be noted that the contact point is only for the hosting providers affected by the removal order. The ABW does not operate a general portal for reporting illegal content on the internet.

Art. 26c. 1. The Head of the ABW shall supervise the implementation of the specific measures referred to in Art. 5(1)–(3) of Regulation 2021/784 by:

1) reviewing the specific measures taken by the hosting provider, including their compliance with Art. 5(2) and (3) of Regulation 2021/784;
2) issuing written recommendations to the hosting provider to remedy the anomalies identified and to bring its operations into line with Regulation 2021/784.

2. An authorised officer of the ABW, when carrying out the activities referred to in paragraph 1, has the right to:

[32] *Punkt kontaktowy TCO* (Eng. Contact point TCO), BIP ABW, https://bip.abw.gov.pl/bip/punkt-kontatowy-tco/525,Punkt-kontaktowy-TCO.html [accessed: 13 XII 2024].

1) enter the controlled premises used for the provision of hosting services;
2) demand explanations from the hosting provider and make available the technical and operational documentation resulting from the application of specific measures or to inspect such documentation.

3. The hosting provider exposed to terrorist content shall remedy the breaches of the law and irregularities identified in the supervision by the Head of the ABW within the timeframe specified in the written recommendation.

Allowing a hosting provider to be subject to specific measures by declaring it vulnerable to terrorist content is linked to the obligation of states to ensure effective oversight functions by competent authorities. As indicated earlier, the safeguards implemented by the hosting provider may relate to appropriate technical and operational measures to enable users to report terrorist content, as well as other mechanisms to raise awareness among content viewers. If, on the other hand, the competent authority considers that the specific measures taken are not compliant, it shall address a decision to the hosting provider requiring it to take the necessary complementary or corrective measures.

To ensure the application of these provisions, it was necessary to indicate that the Head of the ABW shall supervise the implementation of the special measures, which will consist of inspecting the special measures applied by the hosting provider, as well as making written recommendations to the provider in the event that irregularities are found in this regard.

In order to ensure that these activities are carried out, an authorised ABW officer has the right to enter the inspected premises used for the provision of hosting services and to request explanations from the hosting provider and to make available the technical and operational documentation resulting from the application of the special measures.

Under the regulations, the hosting provider is obliged to remedy the irregularities found in a timely manner.

The provisions introduced, on the one hand, refer in some elements to the *Act of 22 August 1997 on the protection of persons and property* and, on the other hand, which is extremely important from the perspective of the principles of the activities implementation, do not exclude the application of the Act – Entrepreneurs' Law.

In the context of the Act on the protection of persons and property, it is worth noting the wording of Art. 43(2) points 3–5, which sets out the principles of the supervision of the Commander-in-Chief of the Police over the activity of specialised armed security formations. The supervision indicated therein consists, inter alia, in entering the premises of an entrepreneur conducting business activity and issuing written recommendations aimed at removing identified irregularities and adjusting the activity of such formations to the provisions of the law.

However, the explanatory memorandum to the Government draft of the Act amending the AT Act and the Act on the ABW and the AW states: *It should be emphasised that the provisions of the Act of 6 March 2018 – Entrepreneurs' Law, including Art. 48, Art. 49(1)–(3) and (6)–(9), as well as Art. 51–57*[33].

In the context of Art. 48 of the Act – Entrepreneurs' Law, attention should be drawn, inter alia, to the obligation of the control authority to notify the entrepreneur of its intention to initiate a control. It shall be initiated no earlier than after the lapse of 7 days and no later than before the lapse of 30 days from the date of delivery of the notice of the intention to initiate control. At the request of the entrepreneur, it may be initiated before the lapse of 7 days from the day of delivery of the notice. A protocol shall be drawn up of the control activities performed in the manner connected with the control.

Pursuant to Art. 49 of this regulation, control activities may be performed by employees of the control body upon presentation to the entrepreneur or a person authorised by the entrepreneur of an official ID card authorising them to perform such activities and upon delivery of an authorisation to perform the control. Its scope cannot go beyond that indicated in the authorisation.

Pursuant to Art. 51–57 of this Act, the control shall be carried out, as a rule, at the entrepreneur's seat or place of business activity and during working hours or while the entrepreneur is actually carrying out business activity. The control activities shall be performed as efficiently as possible and in such a way as not to disrupt the entrepreneur's operations. The findings of the control shall be included in a protocol. In the event that the entrepreneur indicates in writing that the activities carried out significantly interfere with the entrepreneur's business activity,

[33] *Government draft of the Act amending the Act...* – explanatory memorandum..., p. 9.

the necessity to take such activities shall be justified in the inspection protocol. Furthermore, the prohibition to undertake and carry out more than one inspection of the entrepreneur's activity applies. The duration of all controls at the entrepreneur in one calendar year depends on the size of the enterprise. The extension of the duration of the inspection is only possible for reasons beyond the control authority's control and requires justification in writing.

The indicated norms resulting from the Act – Entrepreneurs' Law do not exhaust the entire regulation of control, however, on the basis of the solutions referred to, it should be emphasised that the control of the application of special measures is carried out according to the standard rules provided for the control of entrepreneurs and does not contain distinctive solutions.

Art. 26d. 1. A removal order or a declaration of infringement as referred to in Art. 4(3) and (4) of Regulation 2021/784 shall be given by administrative decision. The provisions of Art. 6, Art. 7, Art. 7b, Art. 8, Art. 12, Art. 14, Art. 16, Art. 24, Art. 26 § 1 and 2, Art. 28–30, Art. 32, Art. 33, Art. 35 § 1, Art. 50, Art. 54–56, Art. 63–65, Art. 72, Art. 75 § 1, Art. 77, Art. 97 § 1 point 4 and § 2, Art. 104, Art. 105 § 1, Art. 112, Art. 113 § 1, Art. 156–158, Art. 217 and Art. 268a of the Act of 14 June 1960 – Code of Administrative Procedure (Journal of Laws of 2024, item 572) shall apply to the proceedings in these cases to the extent not regulated by Regulation 2021/784 and this Act.

2. The designation of hosting providers exposed to terrorist content as referred to in Art. 5 of Regulation 2021/784 shall be carried out by means of an administrative decision. The provisions of the Act of 14 June 1960 – Code of Administrative Procedure, referred to in paragraph 1, and Art. 107 of this Act shall apply to the proceedings in these cases.
3. The decisions referred to in paragraphs 1 and 2 shall be final and immediately enforceable.
4. A hosting provider against whom the Head of the ABW has issued a removal order, or a content provider whose content is covered by a removal order, shall have the right to lodge a complaint against that order with an administrative court within 30 days of:
   1) its delivery in the manner referred to in Art. 3(5) of Regulation 2021/784 – in the case of a hosting provider;
   2) receive the information referred to in Art. 11(1) of Regulation 2021/784 – in the case of a content provider.
5. A hosting provider or content provider against whom the Head of the ABW has issued a decision as referred to in Art. 4(4) of Regulation

> 2021/784 shall have the right to lodge a complaint against that decision with an administrative court within 30 days of receiving notification of that decision.
> 6. A hosting provider against whom the Head of the ABW has issued a decision as referred to in Art. 5(4),(6) or (7) of Regulation 2021/784 shall have the right to lodge a complaint against that decision with an administrative court.
> 7. The complaints referred to in paragraphs 4–6 may be investigated under the simplified procedure referred to in Art. 120 of the Act of 30 August 2002 – Law of the Administrative Courts Procedure (Journal of Laws of 2024, item 935) unless a party requests a hearing and the court considers that all the circumstances of the case have been sufficiently explained and a hearing is unnecessary. The provision of Art. 122 of the Act of 30 August 2002 – Law of the Administrative Courts Procedure shall apply.

In the light of the wording of Art. 26d(1) and (2), a removal order or a finding of an infringement in a cross-border removal order procedure, as well as the designation of hosting providers exposed to terrorist content shall be carried out by means of an administrative decision. The procedural norms for issuing decisions are therefore provided not only by Regulation 2021/784 or the amended AT Act, but also by the *Act of 14 June 1960 – Code of Administrative Procedure* (hereinafter: CAP). The scope of application of the latter Act is, however, significantly limited by the enumerative indication of specific provisions.

Whether indeed such a profound exclusion of the CAP makes it feasible to realistically treat a removal order as an administrative decision may be debatable, especially in the context of the inapplicability in these cases of Art. 107 of the CAP defining the necessary elements of a decision. However, as indicated in the explanatory memorandum to the Act:

> The partial application of the regulations of the Code of Administrative Procedure in this case is necessary. This is based on the fact that the procedure described in Regulation 2021/784 for issuing removal orders is intended to provide a coherent and efficient mechanism at EU level (and therefore across borders) for the removal or blocking of any terrorist content on the network. The effectiveness of this mechanism, in turn, is measured by the speed with which it reacts and performs. As a result, the procedure adopted in the EU instrument with regard to both the issuing of removal orders and the finding of infringements referred to in Art. 4(3) and (4) of Regulation

> 2021/784 differs significantly from some solutions adopted under national administrative law. Moreover, most of the elements within the meaning of the administrative procedure are explicitly laid down in the Regulation itself, e.g. the elements of the decision, the timing and the effect of its notification, and it is therefore necessary to exclude national rules in this case[34].

The explanatory Memorandum to the Act also indicates that the catalogue of provisions of the CAP adopted in Art 26d(1) is modelled on Art. 4(1) of the *Act of 13 April 2022 on specific solutions to counteracting support for aggression against Ukraine and to protect national security*. However, necessary additions and adjustments to the procedure mechanism resulting directly from the provisions of Regulation 2021/784 have been made.

It should therefore be noted that the basic principles of the CAP apply to proceedings for injunctions and the designation of hosting providers exposed to terrorist content (special measures), including:

- the rule of law (Art. 6),
- the principle of objective truth (Art. 7),
- the principle of taking into account the public interest and the legitimate interest of citizens (Art. 7),
- the principle of trust in public authority (Art. 8),
- the principle of swift and simple proceedings (Art. 12),
- the principle of written procedures (Art. 14),
- the principle of permanence of administrative decisions (Art. 16).

The aforementioned provisions are of a strictly guarantee nature from the perspective of protecting the interests of a party. In accordance with Art. 24 of the CAP, the objectivity of the proceedings is also safeguarded by the possibility of excluding an employee of the authority concerned from participating in the proceedings in accordance.

From the perspective of the parties, it is also worth mentioning the application of Art. 28 and 29 of the CAP, according to which a party is anyone whose legal interest or duty is affected by the proceedings or who requests an action of the authority by reason of his/her legal interest or duty. The parties may be natural and legal persons, and when it comes to state and self-government organisational units and social organisations – also units without legal personality.

[34] *Government draft of the Act amending the Act*... – explanatory memorandum, pp. 9–10.

In contrast to the above-mentioned pattern from the Act on specific solutions to counteracting support for aggression against Ukraine and to protect national security, the entire Art. 77 of the CAP applies in the cases covered by the analysed regulation. According to it, the authority is obliged to exhaustively collect and consider all evidence, and may at any stage of the proceedings change, supplement or revoke its decision on the taking of evidence. The body carrying out the procedure at the request of the authority competent to deal with the case (Art. 52 of the CAP) may also, of its own motion or at the request of a party, hear new witnesses and experts on the circumstances which are the subject of those proceedings.

By analogy with removal orders and the finding of infringements in the form of an administrative decision, the designation of hosting providers exposed to terrorist content also takes place, pursuant to Art. 5 of Regulation 2021/784. The CAP also applies to these decisions, but to a limited extent. In this case, however, Art. 107 of the CAP, which is the provision defining the elements of a decision, applies, in contrast to the proceedings related to the issuance of a removal order or a finding of infringement referred to in Art. 4 (3) and (4) of Regulation 2021/748. This is due to the fact that the aforementioned Regulation in this case does not specify the form or components of this decision.

At the same time, in all these cases the proceedings are single-instance and the decisions issued are subject to immediate enforceability, which is related to the need to ensure the efficiency and effectiveness of the conduct of such proceedings. In the context of the single-instance nature of administrative proceedings, Art. 78 of the Constitution of the Republic of Poland should be recalled, according to which each party has the right to appeal rulings and decisions issued in the first instance, and exceptions to this principle and the procedure of appealing are determined by law. Thus, the Constitution of the Republic of Poland allows for such a solution, but it constitutes an exception to the principle, which must have its justification. In these circumstances, it must be sought in the constitutional premise of ensuring public safety and order. For, according to Art. 31(3) of the Constitution of the Republic of Poland, limitations on the exercise of constitutional freedoms and rights, in this case the right to appeal against a decision issued at first instance, may be established only by law and only if they are necessary in a democratic state for its security or public order or for the protection of the environment, public health and morals or the freedoms and rights of others. These restrictions must not affect

the essence of freedoms and rights. In this case, the lack of possibility to appeal against the first instance decision does not seem, in the author's opinion, to violate the essence of the rights referred to above, as the legal action remains. A separate issue, however, is to assess whether this solution is necessary in a democratic state for its security or public order. It also seems to meet this constitutional requirement. While it is conceivable that, as a result of a challenge to the decision, the Head of the ABW will process an application for reconsideration, the substance of the matters decided requires immediate enforceability. A removal order cannot wait until it becomes final, because its essence is to immediately prevent the dissemination of terrorist content. The waiting period for the decision to become final would deprive this legal tool of its preventive significance, as the removal order is not a punishment but a preventive instrument. Only on the basis of other legal provisions in separate proceedings, no longer administrative but criminal, it is possible to punish a provider of such content. An analogous view should be taken of the solution according to which an appeal against the decision would take place to the body of second instance, i.e. the body supervising the formation, in this case the Prime Minister.

The hosting provider against which the Head of the ABW has issued a removal order, or the content provider whose content covers removal order, shall be entitled to lodge a complaint with an administrative court within a period of 30 days. In the first case, this period is calculated from delivery of the decision and, in the second case, from the date of receipt of the information. In this respect, Art. 26d of the Act is an implementation of Art. 9 of Regulation 2021/784, which grants the right to appeal against removal orders issued and other decisions issued by the competent authority.

In case of a hosting provider, the competent authority shall address the removal order to its main organisational unit or to its legal representative. The removal order shall be transmitted to the contact point of the hosting provider by electronic means capable of producing a written confirmation under conditions that allow to establish the authenticity of the sender, including the exact date and time of sending and receipt of the order.

A hosting provider or content provider against whom the Head of the ABW has issued a decision in the aforementioned cross-border removal order procedure shall have the right to lodge a complaint against that decision with an administrative court within 30 days of receiving notification of that decision.

Also, a hosting provider that has been recognised as a vulnerable provider for terrorist content (special measures) has the right to file a complaint against this decision with an administrative court.

Complaints filed in all of the above-mentioned cases may be examined under the simplified procedure referred to in Art. 120 of the *Act of 30 August 2002 – Law of the Administrative Courts Procedure*, i.e. in camera session with three judges, unless a party requests a hearing and the court finds that all circumstances of the case have been sufficiently explained and a hearing is unnecessary. As indicated in the explanatory memorandum to the Act, this solution is intended to ensure that the processing of judicial remedies against decisions is carried out efficiently and effectively, with all guarantees of the right to a court[35].

The procedure adopted in the Act is an administrative procedure. According to the explanatory memorandum to the draft:

> In the proceedings referred to above, the administrative court remains competent court, which is due to the fact that these proceedings will concern exclusively legal-administrative issues. It should be noted that the sanctions set out in Regulation 2021/7 84 relate to situations of failure to comply with certain obligations of an administrative nature by the hosting provider and not their [his/her] commission of punishable acts under the provisions of criminal law substantive law. The mere removal of content is not a sanctioning measure, but a restrictive measure. Accordingly, the draft proponent envisages that, in this respect, only the administrative courts will be the competent judicial units to hear complaints against decisions of the Head of the ABW[36].

In the course of the parliamentary work on the law, another solution was considered to streamline the stage of the ongoing court proceedings. According to it, the transfer of the file and the response to the complaint to the administrative court would take place within 15 days of the receipt of the complaint, while the complaint would be examined by the Provincial Administrative Court within 30 days of the receipt of the file and the response to the complaint[37]. This solution was modelled on Art. 21 of the *Act*

[35] *Government draft of the Act amending the Act...*, p. 11.

[36] Ibid.

[37] *Report of the Administration and the Internal Affairs Committee and the Committee of Digital Affairs, Innovation and New Technologies on the government draft amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence*

of 6 September 2001 on access to public information. The government side, i.e. the draft proponent, reacted negatively to the proposal. It pointed out that it would not guarantee a real acceleration of the processing of possible complaints at the judicial stage, as the deadlines contained therein in relation to the court are instructive in nature.

The governmental side proposed a different solution – consideration by the President of the Republic of Poland of the application of Art. 13 § 3 of the Law of the Administrative Courts Procedure on the basis of which not only the Provincial Administrative Court in Warsaw, but also other Provincial Administrative Courts, e.g. those competent according to the place of residence or seat of the complainant or the place of residence or seat of his/her legal representative, could hear cases concerning complaints against decisions issued by the Head of the ABW. An alternative solution could also be to permanently designate the jurisdiction of Provincial Administrative Court other than the one in Warsaw.

> Art. 26e. A hosting provider, in respect of whom a removal order has been issued, shall communicate to the Head of the ABW data referred to in Art. 21(1) letter (b) and (d) of Regulation 2021/784 by 1 March each year for the preceding year.

The aforementioned Art. 21(1) of Regulation 2021/784 obliges Member States to collect and transmit to the EC, by 31 March each year, the information they have obtained from their competent authorities and hosting providers under their jurisdiction for the previous calendar year. This information , according to Regulation 2021/784 includes:

- the number of removal orders issued and the number of times terrorist content has been removed or access to it has been prevented, and the speed with which removal has taken place or access has been prevented;
- specific measures taken under the Regulation, including the number of times terrorist content has been removed or access to it has been prevented, and the speed with which removal has taken place or access has been prevented;

Agency (print no. 661), print no. 706, https://orka.sejm.gov.pl/Druki10ka.nsf/0/C75A45601BC82E4EC1258BB3003DFB3A/%24File/706.pdf [accessed: 21 XII 2024].

– the number of requests for access made by the competent authorities, in relation to content retained by a hosting provider on the basis of Art. 6 of the Regulation (hosting providers shall retain terrorist content, which have been removed or to which access has been prevented as a result of a removal order or specific measures, which have been removed as a result of the removal of such terrorist content and data which are necessary for: control in administrative or judicial proceedings or for hearing complaints in the event of a decision to remove terrorist content and related data or to disable access to them; or the prevention of terrorist offences, their detection, the conduct of preliminary investigations in their case and prosecution of terrorist offences);
– the number of complaint procedures initiated and actions taken by hosting providers;
– the number of administrative or judicial proceedings initiated and decisions taken by the competent authority in accordance with national law.

Art. 26f. 1. A hosting provider, who fails to comply with the obligation referred to in Art. 3(3) or (6), Art. 4(2) or (7), Art. 5(1–3),(5) or (6), Art. 6, Art. 7, Art. 10, Art. 11, Art. 14(5), Art. 15(1) or Art. 17 of Regulation 2021/784 shall be liable to a fine.

2. The fine referred to in paragraph 1 shall be imposed by the Head of the ABW, by administrative decision, taking into account the conditions and circumstances referred to in Art. 18 of Regulation 2021/784, at a rate of up to 4% of the total turnover of the hosting provider in the preceding turnover year.
3. The decision referred to in paragraph 2 shall be final.
4. The funds from the fines referred to in paragraph 1 shall constitute revenue for the state budget.

Art. 26f contains penalising norms in the form of administrative fines for specific behaviour that constitutes a breach of the obligations set out in Regulation 2021/784. In accordance with Art. 18, Member States shall lay down provisions on penalties applicable in the event of infringements of this legal act by hosting providers and shall take all measures necessary to ensure their enforcement. The enumeration of the articles of Regulation 2021/784, which refer to the obligations of the hosting provider is repeated

after the EU legislator in the described Art. 26f of the Act. A sanction may be applied to a hosting provider in cases where:

- a hosting provider has failed to remove a terrorist content or prevented access to that content in all Member States as soon as possible and, in any event, did so no later than one hour after receiving the removal order (Art. 3(3));
- a hosting provider has failed to inform the competent authority, using the model set out in Annex II to the Regulation, of the removal of terrorist content or the prevention of access to terrorist content in all Member States, indicating in particular the time of that removal or disabling of access (Art. 3(6));
- a hosting provider who has been ordered to remove terrorist content under a cross-border removal order procedure has not taken the measures envisaged for removal orders or has not taken the necessary measures to be able to restore the removed content or access to it (Art. 4(2));
- where the competent authority of the Member State in which the hosting provider has its main organisational unit or where its legal representative is resident or established has issued a decision finding an infringement of the Regulation by an authority of another country which issued a removal order, the hosting provider has not immediately restored the content in question or access to it (Art. 4(7));
- a hosting provider exposed to terrorist content has failed to include in its contractual terms and does not apply provisions to counteract the use of its services for the public dissemination of terrorist content. In doing so, hosting provider shall not act with due diligence, in a proportionate and non-discriminatory manner, taking due account in all circumstances of the fundamental rights of users, in particular freedom of expression and information in an open and democratic society, so as to avoid the removal of material which does not constitute terrorist content (Art. 5(1));
- a hosting provider exposed to terrorist content does not take specific measures to protect its services from the public dissemination of terrorist content (Art. 5(2));
- the specific measures applied by a hosting provider exposed to terrorist content do not meet all of the following requirements:
  - effectively reduce the level of exposure of a hosting provider's services to terrorist content;

  - are targeted and proportionate, taking into account the level of exposure of services to terrorist content;
  - are applied in a manner which fully respects the rights and legitimate interests of users, in particular the fundamental rights of users relating to freedom of expression and information, respect for private life and protection of personal data;
  - are applied in a careful and non-discriminatory manner,
- a hosting provider exposed to terrorist content fails to notify the competent authority of the specific measures he/she has taken and intends to take to comply with its obligations (Art. 5(5));
- a hosting provider exposed to terrorist content has failed to comply with a decision of the competent authority requiring him to take the necessary additional precautionary measures (Art. 5(6));
- a hosting provider has not retained content of a terrorist nature, which have been removed or to which access has been prevented as a result of a removal order or specific measures pursuant to Art. 3 or 5 of the Regulation, as well as the related data which are necessary for the purposes of controlling in administrative or judicial proceedings or the examination of complaints or for the prevention, detection, the conduct of preliminary investigations in their case and prosecution of terrorist offences (Art. 6 of the Regulation);
- a hosting provider has failed to clearly define in its contractual terms its rules against dissemination of terrorist content (Art. 7);
- a hosting provider, who in in the calendar year concerned has taken measures to counter the dissemination of terrorist content or has been required to take action under this Regulation, shall not make a publicly available transparency report on its activities for the year concerned. He shall not publicise the report before 1 March of the following year or the report does not contain the elements provided for in the regulation (Art. 7);
- a hosting provider has failed to establish an effective and accessible mechanism allowing content providers, in case where their content has been removed or access to it has been prevented as a result of specific measures, to submit a complaint against such removal or prevention of access with a request to restore the content or to have access to it (Art. 10);

- a hosting provider fails to process complaints and to restore content or access in a timely manner where their removal or disabling of access was unjustified (Art. 10);
- a hosting provider who has removed terrorist content or has prevented access to it, failed to make available to the content provider of information on such removal or disabling of access or, despite a request from the content provider, failed to inform the content provider of the reasons for the removal or disabling of access and of its rights to challenge the removal order, or failed to provide the content provider with a copy of the removal order (Art. 11);
- a hosting provider, who become aware of terrorist content involving an immediate threat to life did not immediately inform the authority competent for the investigation and prosecution of offences in the Member State or Member States concerned (Art. 14(5));
- a hosting provider has failed to designate or establish a contact point for the receipt of removal orders by electronic means or to ensure that information on the contact point is publicly available (Art. 15(1));
- a hosting provider, which does not have a central organisational unit in the EU, has not appointed a natural or legal person as its legal representative in the EU for the purpose of receiving, complying with and implementing removal orders and decisions issued by competent authorities (Art. 17).

The indicated acts or omissions, despite their large number, do not exhaust the entirety of the behaviour that may be sanctioned on the basis of the catalogue provisions set out in Art. 26f(1) of the Act. However, it is important to emphasise their multidimensionality and the fact that they do not relate solely to the issue of the application of removal orders or specific measures alone, but concern, inter alia, the implementation of obligations relating to the transparency of actions on the part of these suppliers.

The procedure for the imposition of the penalty and its form (by the Head of the ABW by means of administrative decision), as well as the directives for the penalty and its maximum amount has been determined by the legislator in Art. 26f(2). Pursuant to Art. 18 of the Regulation 2021/784 referred to in this provision, the Head of the ABW, when making a decision on the imposition of a penalty and determining its type and amount shall

be obliged to take into account all relevant circumstances of the case, including:

- the nature, severity and duration of the violation;
- the intentionality or negligent nature of the breach;
- the previous infringement committed by the hosting provider;
- the financial condition of the hosting provider;
- the level of cooperation of the hosting provider with competent authorities;
- the nature and the size of the hosting providers, especially whether they are micro, small or medium-sized enterprises;
- the degree of fault of the hosting provider, taking into account the technical and organisational measures taken by him to comply with the requirements of the Regulation.

The maximum administrative penalty adopted in the provision, which may be imposed under the provisions of the Act, also follows directly from Regulation 2021/784. In its Art. 18(3), it is indicated that Member States shall ensure that systematic or persistent failure to comply with the obligations will be subject to fines of up to 4% of the total turnover of the hosting provider in the preceding financial year.

It should further be noted that the Act, as far as the proceedings are concerned, does not exclude or limit the application of the Code of Administrative Procedure. In the result the Head of the ABW will be able to make use of mitigating tools, such as the institution of deferment or payment in instalments. The principle of proportionality is also maintained through the possibility for the authority to apply provisions the authority may waive the fine in favour of a lighter form of punishment, such as a caution, provided that there are legally defined grounds for doing so (Art. 189f of the CAP)[38].

The decisions of the Head of the ABW are of a final nature, therefore also in this non-judicial challenge mechanisms have been excluded.

Funds from fines constitute revenue for the state budget. In this context, it is worth recalling the regulatory impact assessment attached to the draft law, according to which (...) *the draft law provides for the imposition of administrative fines by the Head of the ABW on hosting providers for violations arising from the regulation, which will constitute income to the state budget, revenue to the state budget should be projected from this state budget. However,*

[38] *Government draft of the Act amending the Act...* – explanatory memorandum, p. 13.

it must be assumed that it will be negligible and, moreover, impossible to quantify at this stage[39]. This provision indicates that, in the opinion of the project proponent the actual application of Regulation 2021/784 and the Act itself will be incidental and the level of threat in Poland of dissemination of terrorist content is low. This opinion results from the frequency of application of the solutions from Art. 32c of the Act on the ABW and the AW currently functioning in the Polish legal order.

> Art. 26g.1. In connection with the pending proceedings for the imposing a financial penalty, the hosting provider shall be obliged to provide to the Head of the ABW, at his every request, within 30 days from the date of receipt of the request, the data necessary to determine the basis for the calculation of the financial penalty.
> 2. Where a hosting provider fails to provide data, or where the data provided by that provider makes it impossible to establish the basis of assessment of the financial penalty, the Head of the ABW shall establish the basis of assessment of that penalty on an estimated basis, taking into account publicly available financial data concerning that provider, including criteria referred to in Art. 7(1) points 1–3 of the Act of 6 March 2018 – Entrepreneurs' Law.

Art. 26g obliges the hosting provider to cooperate with the Head of the ABW in relation to pending proceedings for the imposition of financial penalty. Failure to comply with the obligation contained in paragraph 1 or to provide data that makes it impossible to determine the basis for the penalty, shall result in the Head of the ABW determining the basis for the penalty in an estimated manner, taking into account publicly available financial data concerning that supplier, including the criteria referred to in the Entrepreneurs' Law. The criteria mentioned are the size of the company – whether it is a micro-entrepreneur, a small entrepreneur or a medium-sized entrepreneur.

This provision is analogous to the functioning of legal order Art. 101a of the *Act of 10 May 2018 on the protection of personal data*.

[39] *Government draft of the Act amending the Act…* – regulation impact assessment, https://orka.sejm.gov.pl/Druki10ka.nsf/0/5083CA680B1B465AC1258B97003B446F/%24File/661.pdf, p. 8 [accessed: 14 XII 2024].

> Art. 26h. Financial penalty shall be paid within 14 days of the day on which the decision of the Head of the ABW referred to in Art. 26f(2) has become final.

The time limit for payment of the fine shall be 14 days counted from the day on which the administrative decision of the Head of the ABW to impose the fine has become legally binding, and as indicated, it is final.

Summary

With the Act on amending the AT Act and the Act on the ABW and the AW, through the amendment of the AT Act, the proper application of the Regulation 2021/784 was ensured. The designation the Head of the ABW as the Polish competent authority within the meaning of the aforementioned Regulation, as well the establishment of a contact point in the formation headed by him, is optimal from the perspective of improving the functioning of the Polish anti-terrorist system and its division of competences. It should also be regarded as fully justified to base Polish procedural rules, subsidiary to the provisions of Regulation 2021/784, on the solutions adopted in the Code of Administrative Procedure, while acknowledging that in certain cases only its selected provisions may be applicable.

Nevertheless, in the author's opinion, all provisions relevant from the perspective of countering the dissemination of terrorist content on the internet should be transferred to the AT Act, thus Art. 32c of the Act on the ABW and the AW. However, this procedure would only have a legislative dimension, as these regulations contain conflict-of-law rules which guarantee consistency in their application.

Ensuring the application of Regulation 2021/784 by amending the AT Act, in the legislative context, should be complemented with the modification of Art. 1 of this Act, according to which it sets out the rules for the conduct of anti-terrorist activities (therefore, public administration activities) and cooperation between authorities competent to conduct these activities. The solutions adopted in the new chapter 5a of this Act aimed at countering the dissemination of terrorist content on the internet, particularly in the context of the resulting rights and obligations of hosting providers and content providers, should be reflected in the provision defining the scope of the regulation.

From the practical perspective, ensuring the application of Regulation 2021/784 can be assessed as a strengthening of the Polish anti-terrorist system. In this context, it is worth noting that the PERCI platform developed by Europol has been in operation since 3 July 2023. It is a cloud-based solution that ensures the security and protection of the data uploaded to it. This platform facilitates the transmission of removal orders, Member State reporting and coordination, as well as conflict resolution, where there is an ongoing investigation into the content against which the removal order is to be sent[40].

In this context, it should be noted that although according to Regulation 2021/784, countries should ensure its application from 7 June 2022, in Poland this did not happen until 3 December 2024. Until then, Poland was deprived of both formal basis for the application of the Regulation and the possibility to use its technical support tools. This issue remains all the more important as, during this period, alert levels related to heightened threats of a terrorist nature were in force on Polish territory[41].

It is worth to recall in the end the recital 2 of the Regulation 2021/784, which indicates that:

> regulatory measures to counter online dissemination of terrorist content should be complemented by Member States' counter-terrorism strategies, including, inter alia, the strengthening of media literacy and critical thinking skills, the presentation of alternative narratives or counter-narratives and other initiatives to reduce the impact of and vulnerability to terrorist content posted online, as well as investment in social work, deradicalisation initiatives and contacts with the communities concerned, in order to develop sustainable prevention of radicalisation in the society[42].

This guideline, although not obligatory in nature, should be borne in mind in the context of a future assessment of the adopted legislation application. If it turns out that orders or special measures will be frequently

[40] *Government draft of the Act amending the Act…*– explanatory memorandum…, p. 5.

[41] *Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP* (Eng. Alert levels and CRP alert levels introduced so far on Polish territory), Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [accessed: 23 XII 2024].

[42] Recital 2 of the Regulation 2021/784.

applied at the national level, it will become justified to take additional preventive measures.

Bibliography

Burczaniuk P., *Tasks and powers of criminal law enforcement authorities in combating terrorism in Poland – a legal perspective*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 2, pp. 197–219. https://doi.org/10.4467/27204383TER.22.024.16344.

Cichomski M., *Between armed conflict and state terrorism – specific individual restrictive measures adopted in Poland in the context of the war in Ukraine and the situation in Belarus. Legal perspective*, "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 311–350. https://doi.org/10.4467/27204383TER.24.011.19399.

Cichomski M., Idzikowska-Ślęzak I., *Alert levels – practical and legal dimensions of their use*, 2022, "Terrorism – Studies, Analyses, Prevention" no. 2, p. 65, 220–258. https://doi.org/10.4467/27204383TER.22.025.16345.

Cichomski M., Marchliński P., *Krajowe rozwiązania w zakresie bezpieczeństwa obrotu prekursorami materiałów wybuchowych – po zamachu terrorystycznym w Norwegii 22 lipca 2011 r. w kontekście nowych zadań Policji* (Eng. National security arrangements in the trade in explosives precursors – after the terrorist attack in Norway on 22 July 2011 in the context of new police tasks), in: *Polska ustawa Antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (eds.), Szczytno 2016, pp. 591–600.

Gabriel-Węglowski M., *Działania antyterrorystyczne. Komentarz* (Eng. Anti-terrorist activities. Commentary), Warszawa 2018.

Internet sources

Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP (Eng. Alert levels and CRP alert levels introduced so far on Polish territory), Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [accessed: 23 XII 2024].

List of national competent authority (authorities) and contact points, European Commission, 27 I 2025, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en?prefLang=pl [accessed: 15 II 2025].

Punkt kontaktowy TCO (Eng. Contact point TCO), BIP ABW https://bip.abw.gov.pl/bip/punkt-kontatowy-tco/525,Punkt-kontaktowy-TCO.html [accessed: 13 XII 2024].

Legal acts

International Convention on maritime search and rescue, concluded at Hamburg on 27 April 1979 (Journal of Laws of 1988, no. 27, item. 184 and 185).

Treaty on the functioning of the European Union (consolidated version) – (Official Journal of the EU C 202/47 of 7 VI 2016).

Treaty on European Union (consolidated version) – (Official Journal of the EU C 202/13 of 7 VI 2016).

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Official Journal of the EU L 172/79 of 17 V 2021).

Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors (Official Journal of the EU L 39/1 of 9 II 2013).

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Official Journal of the EU L 88/6 of 31 III 2017).

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Official Journal of the EU L 241/1 of 17 IX 2015).

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Official Journal of the EU L 218/8 of 14 VIII 2013).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) – (Official Journal of the EU L 178/1 of 17 VII 2000).

Constitution of the Republic of Poland of 2 April 1997 (consolidated text, Journal of Laws of 1997, no. 78, item 483, as amended).

Act of 18 October 2024 amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency (Journal of Laws of 2024, item 1684).

Act of 26 July 2024 on amending certain acts to improve the activities of the Armed Forces of the Republic of Poland, the Police and the Border Guard in the event of a threat to state security (Journal of Laws of 2024, item 1248).

Act of 17 August 2023 amending the Act – Criminal Code and certain other acts (Journal of Laws of 2023, item 1834).

Act of 7 July 2023 amending the Act – Civil Procedure Code, the Act – the Law on the System of Common Courts, the Act – the Criminal Procedure Code and certain other acts (Journal of Laws of 2023, item 1860).

Act of 7 July 2023 amending the Act on the protection of shipping and seaports and certain other acts (Journal of Laws of 2023, item 1489).

Act of 13 April 2022 on specific solutions to counteracting support for aggression against Ukraine and to protect national security (consolidated text, Journal of Laws of 2024, item 507).

Act of 12 March 2022 on assistance to Ukrainian citizens in connection with the armed conflict on the territory of the country (Journal of Laws of 2022, item 583).

Act of 11 March 2022 on defence of the homeland (consolidated text, Journal of Laws of 2024, item 248, as amended).

Act of 30 March 2021 amending the act on counteracting money laundering and terrorist financing and certain other acts (consolidated text, Journal of Laws of 2021, item 815, as amended).

Act of 21 January 2021 on foreign service (consolidated text, Journal of Laws of 2024, item 1691, as amended).

Act of 10 May 2018 on the protection of personal data (consolidated text, Journal of Laws of 2019, item 1781).

Act of 6 March 2018 – Entrepreneurs' Law (consolidated text, Journal of Laws of 2024, item 236, as amended).

Act of 6 March 2018 – Provisions introducing the Act – Entrepreneurs' Law and other laws on business activity (Journal of Laws of 2018, item 650).

Act of 26 January 2018 – Provisions introducing the Act on the Marshall' s Guard (Journal of Laws of 2018, item 730).

Act of 8 December 2017 on the State Protection Service (Journal of Laws 2018, item 138).

Act of 16 November 2016 – Provisions introducing the Act on the National Revenue Administration (consolidated text, Journal of Laws of 2016, item 1948, as amended).

Act of 10 June 2016 on anti-terrorist activities (Journal of Laws of 2024, item 92, 1248, 1684).

Act of 13 April 2016 on the security of trading in explosives precursors (consolidated text, Journal of Laws 2019, item 994).

Act of 30 August 2002 – Law of the Administrative Courts Procedure (consolidated text, Journal of Laws of 2024, item 935, as amended).

Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence (consolidated text, Journal of Laws of 2024, item 812, as amended).

Act of 6 September 2001 on access to public information (consolidated text, Journal of Laws of 2022, item 902).

Act of 6 June 1997 – Criminal Code (consolidated text, Journal of Laws of 2024, item 17).

Act of 6 April 1990 on the Police (consolidated text, Journal of Laws of 2024, item 145, as amended).

Act of 14 June 1960 – Code of Administrative Procedure (consolidated text, Journal of Laws of 2024, item 572).

Regulation of the Prime Minister of 20 June 2002 on "the Principles of Legislative Techniques" (consolidated text, Journal of Laws of 2016, item 283).

Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online (Official Journal of the EU L 63/50 of 6 III 2018).

Case law

Judgement of the European Court of Human Rights in the case Pietrzak v. Poland and Bychawska-Siniarska and Others v. Poland, https://arch-bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/orzecznictwo-europejskiego-trybunalu--praw-czlowieka/listByYear,2.html?ComplainantYear=2024 [accessed: 18 V 2025].

Other documents

Commission Staff Working Document Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12 IX 2018, SWD(2018) 408 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN [accessed: 4 V 2023].

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms, Brussels, 28 IX 2017, COM (2017) 555 final.

Mechanisms for blocking terrorist content on the internet in the light of the Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, Presentation by the Ministry of Internal Affairs and Administration, prepared for the Interministerial Team for Terrorist Threats.

Government draft amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency, print no. 661, https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=661 [accessed: 24 XII 2024].

Report of the Administration and the Internal Affairs Committee and the Committee of Digital Affairs, Innovation and New Technologies on the government draft law amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency (print no. 661), print no. 706, https://orka.sejm.gov.pl/Druki10ka.nsf/0/C75A45601BC82E4EC1258BB3003DFB3A/%24File/706.pdf [accessed: 21 XII 2024].

Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, Brussels, 14 II 2024, COM(2024) 64 final.

The European Commission's position on 9 June 2021 (ref. no. INFR(2021)2046, C(2021)3630 final).

Mariusz Cichomski

Lawyer, sociologist. He works on issues related to terrorism, organised crime, oversight of service activities, security legislation and issues related to the application of restrictive measures. He is the author of more than 30 publications on security, particularly in the legal dimension, and on sociology.