DOI: 10.38146/BSZ.2024.1.8

Procedural dilemmas of cybercrimes involving illegal content dissemination in cross-border situations[1]

Kinga Sorbán
PhD, assistant research fellow
University of Public Service,
Institute of the Information Society
kinga.sorban@gmail.com

Abstract

Aim: The main purpose of this study is to provide a comprehensive overview of the procedural dimensions of the investigation of cybercrimes having an international element. In this context, it highlights the difficulties that can slow down and, in extreme cases, even prevent effective enforcement in two major areas: jurisdiction and mutual legal assistance.
Methodology: As the study primarily focuses on legislative approaches, it brings together and comparatively analyses the main EU and international legal sources that regulate cooperation between countries in the field of cybercrime.
Findings: Especially in the area of mutual legal assistance, the European Union is actively legislating, and the principle of indirectness, i.e., the possibility for the competent authorities to directly contact intermediary service providers established in another Member State, is increasingly gaining prominence. On one hand, this can speed up procedures, but on the other hand, it entails the risk that the numerous instruments overlap, weakening the effectiveness of enforcement.
Value: As some of the legislative procedures are still underway, further research is needed to see how Member States will be able to apply the new instruments in practice.

Keywords: cybercrime, international cooperation, jurisdiction, mutual legal assistance

1 Jelen angol nyelvű cikk a magyar változat utánközlése. DOI link: https://doi.org/10.38146/BSZ.SPEC.2024.1.1. A cikk a szerkesztőséghez magyar nyelven érkezett be.

Introduction

Crimes committed in the online space are seldom linked to only a single country. In the case of content crimes, the possibility of the perpetrator and the victim being in different countries is not inconceivable, while it is extremely rare for large-scale malware infections to impact the information systems of just one country.[2] Nowadays, it is common practice to host web servers in countries where the capacity of investigative authorities to detect the incident is low: the UN Conference on Trade and Development in 2020 highlighted that developing countries are lagging behind in criminalising and prosecuting cybercrime (URL1). In the case of cybercrime, an international element can be attached to almost any aspect of the crime, which makes international cooperation a priority.

Despite cybercrime's international nature, international cooperation still faces many difficulties, as Kitti Mezei points out that Kitti Mezei points out that two-thirds of cases in which electronic evidence is located abroad are impossible to prosecute properly (Mezei, 2022).

The investigation of cybercrimes with an international dimension has two critical points: one is the establishment of jurisdiction and the other is the conduct of procedural acts abroad, mutual legal assistance. My study deals with these two issues. As both jurisdiction and legal assistance are governed by extensive sets of international rules, my main aim is to provide an overview of the legal instruments available in proceedings with a foreign dimension. I pay particular attention to the principle of extraterritorial jurisdiction, which has been promoted in recent years by the European Union through legislation, enabling law enforcement authorities in one Member State to carry out procedural acts directly in another Member State. The EU legal framework provides this possibility mainly when an internet intermediary service provider is involved in the procedure. These online service providers may store important pieces of evidence or take steps to render allegedly illegal content inaccessible for the duration of the proceedings. The most popular online service providers are typically not based in Hungary (for example, the European headquarters of Meta, which operates Facebook, is located in Ireland), so if they are involved in domestic proceedings investigating authorities must necessarily apply the rules of international cooperation.

2 Today's popular malicious software can infect people all over the world. According to the security firm Kaspersky, the WannaCry ransomware virus has infected around 230 000 computers in 150 countries.

Jurisdiction in the fight against cybercrime

Jurisdiction is essentially the guiding principle which determines the distribution of cases between states, i.e. which country's authorities and courts have the right and duty to act. In Hungarian domestic law, the provisions of Act C of 2012 on the Criminal Code (hereinafter: the Criminal Code) reflect the principle of territoriality, according to which the criminal jurisdiction of the Hungarian state extends to acts committed on the territory of the country.[3] It also knows the active personality principle (also known as principle of nationality) principle, according to which Hungarian jurisdiction shall be established over acts committed by Hungarian nationals abroad if it constitutes a criminal offence under Hungarian law.[4] As supplementary principles, the Criminal Code sets out the protective principle (under which an act is subject to Hungarian jurisdiction if it constitutes a criminal offence against the state),[5] and the principle of universal jurisdiction (in the case of crimes against international law, Hungarian courts' jurisdiction is also provided for). Another additional principle relevant to our topic is the so-called passive personality principle, according to which Hungarian jurisdiction can be established over acts committed abroad by non-Hungarian citizens if the victim is a Hungarian citizen andthe act is punishable under Hungarian law.[6] These jurisdictional rules are traditionally tailored to acts committed in physical space, e.g., if a dead body is found with a knife the chest by the police, the place of the crime is evident or at least easily ascertainable while the perpetrator is assumed to have been present. The situation is much less straightforward when it comes to the online space, where determining the place of the commission of the offence can cause major challenges. Let's take hate speech as an example to illustrate the questions that arise upon determining the place of commission: is it the place of residence of the person who is making the statement or the place where the person concerned resides and where there is an imminent threat of violence? Perhaps is it the country where the server hosting the post is located, or the country of establishment of the social media platform owning the server?

These are not easy questions, and the provisions of Hungarian law do not provide clear answers. Given the specific nature of cybercrime, there are a number of international treaties and EU legal instruments that have provisions on jurisdiction, which I will explore below.

3 CC. § 3 Paragraph (1) Point a)-b).
4 CC. § 3 Paragraph (1) Point c).
5 CC. § 3.
6 CC. § 3 Paragraph (2) Point b).

Jurisdiction in international law

Article 22 of the Convention on Cybercrime,[7] which was 20 years old in 2021, regulates jurisdiction. Similarly to the national laws of the States Parties, the Cybercrime Convention gives primacy to the principle of territoriality, i.e. the jurisdiction of the State extends to offences committed in its territory.[8] As a secondary connecting factor, the Cybercrime Convention applies the active personality principle,[9] i.e. if if it is not possible to determine which country has jurisdiction on the basis of the principle of territoriality, the state in which the offender is a national is also permitted to act.

However, applying the principle of territoriality in practice can cause difficulties, as the Cybercrime Convention does not provide guidance to the States Parties on its application. As the previous questions on hate speech illustrate, locating the perpetrator in the online environment is not a simple task. The application of the principle becomes more problematic if the countries that are competent to prosecute have different perceptions of the location where the offence was committed, as this can result in either a positive (several countries want to prosecute) or a negative (no country wants to prosecute) conflict of jurisdiction. As a criticism of the principle of territoriality, Dávid Tóth and Zsolt Gáspár argue (Tóth & Gáspár, 2020) that there are several cases where no prosecution is brought in the country of the place of the commission of the offence (i.e. the country in which the offender carries out the act), since there were no victims in the territory of that country.In addition, by using a VPN, the perpetrator can easily spoof location systems, which based on the IP address used, link the offence to a completely different country than the one where it actually took place.

The principle of dual criminality can also be an obstacle to prosecution. The principle of double criminality is the requirement whereby the act of a foreign national can only be punished if it is a criminal offence under the law of both the country seeking prosecution and the country in which the offender is a national (Blaskó & Budaházi, 2019). This universal principle of law isa general condition for international criminal cooperation (Kondorosi & Ligeti, 2008) and is

7 Act LXXIX of 2004 on the promulgation of the Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001.
8 Article 22 Point 1 Subpoint a)-c).
9 Article 22 Point 1 Subpoint d).

applied in some form by most countries;[10] as such it may pose a potential challenge in criminal proceedings where an offender's actions cause serious harm but are committed in a country where they do not amount to a criminal offence.

The principle of double criminality was an obstacle to the prosecution of the LoveBug malware (Rawat, 2021; Brenner, 2006). In the 2000s, a virus that sent masses of infectious emails with the message 'ILOVEYOU' spread like wildfire across the internet. The virus overwhelmed the entire Internet network quickly and filled the entire corporate mailboxes of several large corporations, causing roughly eight billion dollars of damage. The creator of the LoveBug malware was tracked down swiftly by the investigating authorities: a university student in the Philippines claimed to have accidentally unleashed the virus on the Internet. Despite the huge amount of damage, in the 2000s the Philippines did not have a law to criminalise the distribution of malware. The local prosecutor's office investigated the possibility of prosecuting the offence as the fraudulent useof non-cash payment instruments, but concluded that it was unrelated to the interference with computer systems. As there was no double criminality, the perpetrator was ultimately not charged and went unpunished (URL2).

Applying the passive personality principle, relying on the nationality of the victim, as a secondary connection principle can lead to conflicts in cases with numerous victims across multiple countries (for example, in the event of a widespread malware infection that infects computers in several countries).

Issues with jurisdiction are not limited to the prosecution of the offender, but also arise when it comes to the enforcement of decisions especially when illegal content is hosted on the server of a provider located outside the EU.In this case, the enforcement of a court or other authority's decision to remove the content or other forms of electronic data temporarily or permanently depends solely on the goodwill of the service provider.

In the Yahoo case,[11] a jurisdiction issue arose over the enforceability of a court decision. The main issue raised in the case was whether US courts should facilitate the enforcement of judgments delivered by non US courts against overseas subsidiaries of US-based companies. In France, for example, the use of authoritarian symbols is forbidden,[12] and a French court deemed the sale of Nazi artifacts in online auctions illegal. The French anti-discrimination non-profit organisation

10 The international conventions mainly refer to the principle of double criminality in the context of extradition and mutual legal assistance. The EU Framework Decision 2002/584/JHA makes extradition in EU Member States conditional on double criminality, i.e. that the offence is a criminal offence in both the requesting and the extraditing country.

11 Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme.

12 Code Pénal Article R645-1.

La Ligue Contre Le Racisme et l'antisemitisme has filed a lawsuit against auction site Yahoo for allowing French users to view such auctions and bid on the items posted on the site. As a defence, Yahoo claimed that as an American company it was not subject to French law, but the French court disagreed and imposed a fine of one thousand francs. The French court argued that if France is the country of destination of the service, then French law must be complied with and the auctions in question must be removed or made inaccessible to users who use French IP addresses. The French authorities have contacted the United States to enforce the court's decision, and Yahoo has filed a lawsuit in response. Claiming a violation of the First Amendment guaranteeing freedom of speech, the company argued that the implementation of the French court's ruling in the US would lead to a violation of the freedom of speech of US users, as US law does not prohibit the use of authoritarian regimes, including the sale of Nazi memorabilia on the internet.

The 9th Circuit Court acting as an appellate forum, ultimately concluded that US courts did not have jurisdiction to rule on a lawsuit against a French organisation, and the issue was not even taken to the merits. Such jurisdictional problems will naturally result in the unenforcability of domestic court decisions in foreign countries.The problem, according to Brenner and Koops, is not the existence of jurisdictional disputes between countries, but rather the lack of a common mechanism to determine the country with the closest connection to the act, thus resolving the conflict (Brenner & Koops, 2004). The Cybercrime Convention merely proposes that countries resolve disputes through consultation,[13] without imposing any legal consequences for failure to do so. It may therefore be appropriate to consider the establishment of an international body competent to decide on similar issues, or at least to which States Partiesto the Cybercrime Convention may refer for guidance.

Jurisdiction in the European Union

In the European Union, the rules of jurisdiction are more complex, with EU legislative instruments laying down specific rules for each type of offence. In the following section, I will provide an overview of the jurisdictional provisions in the law of the EU in relation to cybercrime, including cybercrime committed over networks.

Directive 2013/40/EU addresses jurisdictional issues for computer crimes in the narrow sense (unauthorised access, system interference and misuse of

13 Cybercrime Convention Article 22 point 5.

data). According to Article 12 of the Directive, the principles of territoriality and nationality both apply, which means that a Member State shall establish its jurisdiction when the offence is committed in whole or in part within its territory and also when it is committed by one of its nationals. The Directive – correctly – interprets the place of commission in a broad sense, as it addresses a recurring problem, namely that in the case of offences committed in virtual space, the offence may in fact be committed in several places at the same time. According to the Directive, an offence is deemed to have been committed on the territory of a Member State if the offender is physically present on its territory at the time of commission of the offence but also if the offender is elsewhere but the information system against which the offence is committed is located on its territory. Extending the interpretation of the place of commission could lead to a situation whereseveral Member States consider the offence to have been committed on their territory at the same time. This typically occurs when the offender and the information system concerned are located in different Member States, but it is also possible when targets are located in several other countries in addition to the Member State of the physical location of the perpetrator (e.g. when spreading a computer virus). In such situations, it is for the Member States to negotiate which of them will prosecute the case, although it is recommended to opt for the jurisdiction of the Member State having the closest connection to the case. Directive 2011/93/EU criminalises child pornography and grooming in the Member States. To ensure effective prosecution of criminalised offences, the Directive also lays down common rules for establishing jurisdiction. The combined application of the principles of territoriality and nationality has primacy for determining jurisdiction. A Member State may conduct proceedings if the offence was committed in whole or in part within its territory[14] or if the offender is one of its nationals.[15] As a complementary principle, Member States have discretion to establish their jurisdiction even if the above conditions are not met. This may happen in the following cases:

- the victim is a national or a person who is an habitual resident in that Member State,
- the act was committed for the benefit of a legal person established in that state, and
- the offender is an habitual resident in that Member State.[16]

14 Directive 2011/93/EU Article 17(1)a).
15 Directive 2011/93/EU Article 17(1)b).
16 Directive 2011/93/EU Article 17(2).

As the victims of these offences are minors, it is appropriate and reasonable to allow the Member State of the victim's nationality to prosecute.Proceedings in a foreign language, possibly in a distant country, foreign and even repeated procedural acts (for instance witness hearings) can result in the multiple traumatisation of the victim, whose main interest is to have the proceedings in the place closest to him/her, in a familiar and safe environment. The Directive also erodes the principle of double criminality by stipulating that the jurisdiction of the Member State is not subordinated to the condition that the acts are a criminal offence at the place where they were committed.

Directive 2019/713/EU regulates the fraudulent use of non-cash payment instruments, including corporeal and non-corporeal instruments and fraud related to information systems. The provisions establishing jurisdiction do not differ from those found in other EU legal instruments on cybercrime, so the principles of territoriality and nationality are shall prevail.[17]

Mutual legal assistance for cybercrime

If an act has a foreign element, it is often necessary to seek the help of a court or administrative authority of another country to perform the necessary procedural steps; this is called mutual legal assistance. Mutual legal assistance does not have uniform rules of procedure applicable to all countries, bilateral or multilateral treaties regulate such relations between countries and set out the rules that apply to different areas of law. These mutual legal assistance treaties do not generally focus on specific forms of offences, instead they address the main procedural elements of cross-border investigations, which require cooperation.[18] Hence, one will not find any criminal procedural rules in these mutual legal assistance treaties that address the specific characteristics of cybercrime, such as the volatile nature of evidence in the online space. At the same time, the proliferation of electronic communications today is making it difficult to imagine a crime that does not leave some kind of trace in cyberspace or in the systems of a telecommunications service provider. The provisions on obtaining evidence in mutual legal assistance treaties therefore necessarily addressthe acquisition, retention or removal of of data stored by telecommunication or other information society service providers is some form.

17 Directive 2011/93/EU Article 12(1).

18 For example, Act XL of 2006 on the proclamation of the treaties between the Government of the Republic of Hungary and the Government of the United States of America amending the treaties on extradition and mutual legal assistance in criminal matters signed in Budapest on 1 December 1994.

Mutual assistance between the Member States of the European Union

The rules on criminal cooperation between EU Member States are set out in the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[19] (hereinafter the Mutual Assistance Convention).[20] As it is an international convention and not a classical source of EU law, its adoption required ratification by the Member States (Villányi, 2003). One of the most significant achievements of the Mutual Assistance Convention is that it enables judicial authorities of the Member States to contact each other directly or the purpose of providingmutual legal assistance in criminal matters. Formerly, this was possible only through the involvement of the Ministries of Justice, which slowed down procedures dramatically.

The Mutual Assistance Convention is not intended to be a complete, comprehensive set of rules on mutual legal assistance between EU Member States; this is clearly reflected in Article 1, which states that the Mutual Assistance Convention is intended to supplement the rules of other international conventions in order to make cooperation in this area more effective. The Mutual Assistance Convention supplements the rules of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, its Additional Protocol of 17 March 1978, the 1985 Schengen Implementation Conventionand the Benelux Treaty, therefore its provisions cannot and must not be interpreted and assessed independently, but in conjunction with the provisions of the aforementioned conventions. The Mutual Assistance Convention also stipulates that if there are bilateral or multilateral agreements between Member States that are more favourable than the rules of the Mutual Assistance Convention, these take precedence and may supersede the rules of the Convention.

Mutual assistance between EU Member States and third countries

Mutual assistance between EU Member States and third countries is still possible through the central authorities (the Ministry of Justice in Hungary), yet this is not only time-consuming but also resource-intensive.

19 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union.

20 Act CXVI of 2005 on the proclamation of Council Act of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and the Additional Protocol to the Convention on 16 October 2001.

Requests for mutual assistance concerning evidence often arise during the investigation phase of criminal proceedings. In a cyberspace setting, the relevant tools for gathering evidence from remote locations are to order the preservation and disclosure of data. The Cybercrime Convention' procedural provisions set minimum standards for electronic evidence, which each State Party must implement into its own legal system. Under the Cybercrime Convention, States Parties should be able to order expeditious preservation of specified computer data (including traffic data) stored on the system,[21] as well as to issue production orders in order to oblige persons in their territory to submit computer data stored in a computer system or a storage medium in their possession, and to oblige service providers to submit subscriber information and traffic data. The Cybercrime Convention has specific provisions on mutual legal assistance in the area of cybercrime,encouraging the widest possible cooperation between States Parties in this area. The Cybercrime Convention is not intended to replace bilateral mutual assistance treaties, and thus states that where a mutual assistance treaty is in force between two States, that shall prevail during the investigation and gathering evidence. However, if there are two countries that are parties to the Cybercrime Convention but there is no mutual assistance agreement between them, they are bound by the rules of the Cybercrime Convention. States Parties are obliged to designate central authorities to deal with requests for mutual assistance, including sending, receiving and responding to requests for assistance in relation to cybercrime, including cybercrime committed over networks. Under the rules on mutual assistance of the Cybercrime Convention, the following measures may be requested from a State Party as per the mutual assistance rules:

- expedited preservation of stored computer data,
- expedited disclosure of preserved traffic data,
- mutual assistance regarding accessing of stored computer data,
- mutual assistance in the real-time collection of traffic data,
- mutual assistance regarding the interception of content data.

Yet the Cybercrime Convention's rules do not specify the types of traffic data that states must store nor the duration of storage, so there is a wide variety of regulatory solutions when looking at countries that are not members of the European Union. The popularity of cloud services also puzzles investigating authorities, as the essence of cloud storage is that the same piece of data can be present in multiple countries on multiple servers. This can occur either by having multiple copies of the whole of the data subject to the criminal proceedings on multiple

21 Cybercrime Convention Article 16.

servers, or by having fragments of the data scattered across servers.In the United States, the case of United States v. Microsoft Corp.[22] addressed the issue of whether a service provider established in one country is obliged to disclose data when the data requested by an investigating authority is stored in another country. In the United States, the investigating authority asked the company to produce certain data in connection with a drug smuggling case. Microsoft disclosed the relevant traffic data but not the content data (email messages), claiming that it was stored in its data centre in Ireland. The US Court of Appeals for the 2nd Circuit Court ruled that such warrants apply only within the territorial jurisdiction of the United States. The Supreme Court eventually rendered the judgment moot and suggested the investigating authority to issue a new warrant, because in the meantime Congress had passed a law on cloud services (Clarifying Lawful Overseas Use of Data Act – CLOUD Act), which makes the disclosure of data mandatory even if stored abroad. An interesting aspect of the caseb is the amicus curiae filed by Ireland, where the data in question was stored, arguing that the transfer of the data to a third country are in violation of the EU General Data Protection Regulation (GDPR) as well as Irish law, as the data should have been requested by the US authorities under the rules of the US-Ireland Mutual Legal Assistance Treaty, not directly from the company (URL3). Moreover, the European Data Protection Board considers the CLOUD Act rules to be in conflict with EU law (URL4), notwithstanding the fact that the EU itself, as discussed below, emphasises the principle of immediacy in cross-border evidence.

Extraterritorial jurisdiction instead of mutual legal assistance: measures directly applicable to service providers under the jurisdiction of another Member State

Cybercrime, the volatility of evidence and the mobility of offenders require certain procedural steps to be taken expeditiously. As a general rule, where evidence is to be collected or coercive measures are to be taken abroad, the procedure is carried out by the foreign country having jurisdiction over the person or entity concerned, on request of the Hungarian authorities. However, where procedures involve a multiple-step process, rapid action cannot be ensured.There is a growing need for investigating bodies to be able to carry out certain procedural acts directly in another Member State without involving the authorities of this Member State, or rather by simply informing them. The concept of extraterritoriality in enforcement is not unique, as it is possible to enforce decisions abroad on the

22 United States v. Microsoft Corp., 584 U.S., 138 S. Ct. 1186 (2018).

basis of a directly applicable binding acts of the European Union with general application, statutes, government regulations or reciprocity (Boros, 2016). The need has now evolved into an EU-wide effort to simplify the collection of evidence between Member States, the enforcement of coercive measures and the implementation of certain measures, through active legislation.

In the following section, I will examine the situations where it is possible to take direct action beyond the borders of Hungary during criminal proceedings, based on the three main categories of measures that are also covered by the rules on mutual legal assistance in the Cybercrime Convention. First, I will compare the rules that govern requests for data. Then I look at the instruments for preserving digital evidence and finally at the instruments for removing or rendering inaccessible unlawful information.

Requesting internet intermediary service providers established in another Member State to disclose information

In criminal proceedings, the purpose of requests for information is to enable investigating authority to obtain information about the suspect, potential witnesses, the circumstances of the commission of the offence or to gather evidence. It is possible to request information from domestic intermediary service providers under § 261 of the Code of Criminal Procedure (CCP), with the limitation that intermediary service providers that qualify as electronic communications service providers (e.g. internet service providers) can only be requested to provide information upon authorisation by the public prosecutor. However, the rules of the Hungarian CCP only apply to service providers under Hungarian jurisdiction; if the service provider storing the information is established under a different jurisdiction, the mutual assistance instruments shall be sought. The EU's E-evidence draft regulation will bring a major change in this area, as it would introduce European production orders, on the basis of which a Hungarian court, prosecutor's office or authority could directly oblige service providers established in other Member States to disclose data.

A new and already applicable instrument in the regulatory palette is order to provide informationintroduced by the Digital Services Act (DSA).[23] It is not an instrument of criminal proceedings, intended use is to ascertain whether individual users of the service are engaging in law-infringing conduct through the service. Although it covers infringements of a criminal nature, it is not limited to them. Accordingly, the authority issuing the order is not necessarily a judicial

23 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

authority, and Member States may even confer the power to issue such orders on an administrative authority. The provider is obliged to inform the issuing authority of the receipt of the order and whether it has been executed,[24] suggesting that the provision of information on the user is not mandatory. This assumption, however, is contradicted by once of the recitals of the DSA, which provides that *'in the event of non-compliance with such orders, the issuing Member State should be able to enforce them in accordance with its national law'*.[25] Nevertheless, if important information is needed in a criminal matter, tissuing orders to provide information is discouraged. It is also an open question whether the information thus obtained can be used as evidence in criminal proceedings.

The upcoming regulation on European Production and Preservation Orders for electronic evidence in criminal matters, to be introduced as part of the European e-Evidence package would also include an instrument for providing information. This, unlike the DSA's order to provide information, could only be issued by an authority competent to act in a criminal matters, while the provision of information would be mandatory for the requested service provider. Katalin Parti's publication highlights the need to revise Hungarian legislation in light of the adoption of an EU legal act itroducing European production orders. As things stand at present, the adoption of the regulation may lead to a situation where service providers will be obliged to comply with foreign request under EU law, while while domestic law explicitly prohibits it from doing so, example.g. if the information requested is classified (Parti, 2018).

Table 1
Instruments to request the provision of information in EU law

	DSA orders to provide information	European production order (e-evidence package)
Issuer	National judicial or administrative authority.	Judge, court, prosecutor, competent authority in criminal proceedings.
Subject	An intermediary service provider established in any Member State: - mere conduits, - cache provider, - hosting provider, - online platform, - video sharing platform.	Electronic communications service providers, information society service providers where data storage is a key element of the services provided to the user (social networking sites, online marketplaces and other hosting providers), internet domain name providers and IP numbering providers.
Aim	To determine whether the recipients comply with EU or national law.	To obtain evidence and identify the perpetrator in criminal proceedings.
Mandatory force	Not mandatory.	Mandatory.

Note. Table prepared by the author.

24 DSA Article 10(1).
25 DSA recital (32).

Instruments to preserve information in EU and national law

Imposing data retention and preservation obligations on service providers, either in general or in specific cases, is intended to ensure the integrity and preservation of electronically stored evidence. The efficiency of the evidentiary process is hampered if such data are removed, altered or deleted. Hungarian law in effect provides for the retention of traffic data generated in the course of the provision of communications services, it grants the possibility to impose an individual preservation obligation for other types of data. However, these are measures that can be imposed on service providers under Hungarian jurisdiction. General data retention in relation to communications data was recognised by the EU preceding the Digital Rights v. Seitlinger case, where the European Court of Justice ruled that such an extensive obligation to retain data would restrict citizens' right to privacy to an extent that is disproportionate compared to the most serious law enforcement interest and declared the relevant part of the ePrivacy Directive invalid. The revision of the e-Privacy Directive is currently in progress, and as such the current EU law does not provide for a general data retention obligation. Member States can of course prescribe such obligations in their national law, but the result will be the lack of common rules on the data types that European service providers shall store and on the length of time for which they may store them; this fragmented legal environment will eventually jeopardise the success of cross-border investigations.

Currently, only terrorist content is subject to an individual preservation obligation, which is imposed only on hosting providers. They are required not only to remove information identified as terrorist content, but also to preserve it so that it can be used in criminal proceedings.

A similar obligation would be introduced in a new regulation on combatting child sexual abuse, where preservation would not be mandatory, but voluntary.

To complement the rules in this area, the e-Evidence package would introduce mandatory European preservation orders, which can be used to impose an obligation on the service provider of another Member State to preserve information relevant to the procedure.

Table 2
Data preservation instruments in EU law

	European Preservation Order (e-Evidence package)	Information preservation under the draft regulation on child sexual abuse	Preservation of content and related data under Regulation 2021/784
Issuer	Judge, court, prosecutor, competent authority in criminal proceedings.	–	–
Subject	Electronic communications service providers, information society service providers where data preservation is a key element of the service provided to the user (social networking sites, online marketplaces and other hosting providers), internet domain name providers and IP number providers.	Hosting service providers and providers of interpersonal communications services.	Hosting service providers.
Aim	Prevent the removal, deletion or alteration of data.	Preservation of relevant data as evidence for the purpose of subsequent obligation to provide.	Preservation of removed or inaccessible terrorist content to be able to comply with a subsequent production order.
Mandatory force	Mandatory.	Voluntary.	Mandatory.

Note. Table prepared by the author.

Instruments to remove illegal content or render them inaccessible

Two other important compulsory measures in cross-border criminal proceedings should be mentioned. For crimes involving illegal content dissemination, in addition to ensuring that the authorities preserve evidence, they there is a need to ensure Internet users's discontinued access to content that is deemed illegal. This can be achieved by removing the data in question or rendering it inaccessible. The difference between the two instruments is that, upon removal, the content in question is deleted from the hosting server, but upon rendering it inaccessible, its location of the problematic content remains unchanged, yet users or a group of users loose access thereto. Removal is typically the responsibility of the hosting provider on whose server the content is stored, while blocking access can also be achieved through other intermediary service providers, because internet service providers can also make certain domains inaccessible to their users. Compulsory measures to render electronic data inaccessible permanently or temporarily shall be applied in accordance with Section 335 of CCP to service providers under Hungarian jurisdiction.

Service providers not established in Hungary can be ordered to remove illegal content in general pursuant to the DSA[26] and while to removing terrorist content Regulation 2021/784 shall be applied. The DSA orders to act against illegal content, similarly to orders to provide information, are not traditional instruments of criminal law, as they can be applied to any type of unlawful content, for example in consumer protection cases. The recital to the DSA also explicitly provides for the relationship between orders and instruments of criminal procedure by stating that the rules of the DSA *'might not apply'* and *'mightbe adapted'* in cases where the Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal matters, regulations addressing specific types unlawful content and the provisions of international civil and criminal law provide for different conditions.[27] A typical example is Regulation 2021/784 on terrorist content, where the hosting provider is obliged to remove the content within one hour of receiving the request, but if adopted; the same approach is enshrined in the proposal for a regulation on child sexual abuse.

Table 3
Instruments for removing illegal content in EU law

	DSA orders to act against illegal content	Removal orders based on draft regulation on child sexual abuse	Removal orders under Regulation 2021/784
Issuer	National judicial or administrative authority.	At the request of the coordinating authority, the judicial or administrative authority of the Member State of establishment.	Competent authority of the Member State.
Subject	An intermediary service provider established in any Member State: - mere conduit, - cache provider, - hosting provider, - online platform, - video sharing platform.	Hosting service providers.	Hosting service providers.
Aim	To remove illegal content.	To remove content identified as child sexual abuse material.	To remove terrorist content.
Mandatory force	The provider shall inform the issuer of any effect given to the order. If not, implementation can be initiated at national level.	Mandatory, within 24 hours.	Mandatory, within one hour of receiving the removal order.

Note. Table prepared by the author.

26 According to recital (34) of the DSA, the national authorities concerned should be able to issue orders against content deemed to be illegal and to address them to intermediary service providers, including those established in other Member States.
27 DSA recital (34).

Table 4
Instruments for making illegal content inaccessible under EU law

	Disable Access under the Draft Regulation on Child Sexual Abuse	Disable Access under Regulation 2021/784
Issuer	At the request of the coordinating authority, the judicial or administrative authority of the Member State of establishment.	Competent authority of the Member State.
Subject	Internet access service provider.	Hosting service providers.
Aim	To block users from having access to known child sexual abuse content.	To prevent users from having access to terrorist material.
Mandatory force	Mandatory, start and end dates are set by the coordinating authority.	Mandatory, within one hour of receiving the removal order.

Note. Table prepared by the author.

Conclusion

In this study, I have examined two areas of international cooperation where action against cybercrime is more challenging. Jurisdiction, as the framework governing the allocation of cases between countries, can hardly be influenced through classical forms of regulation, due to its bilateral treaty-based nature and the limited number international laws. Apart from the jurisdictional rules that underpin the allocation of cases, the focus lies primarily on the cooperation between countries. Of course, mechanisms can be developed to encourage cooperation, such as a body to facilitate resolving either positive or negative jurisdictional conflicts between countries.

Regulation has a much greater role to play when a cross-border procedural activity needs to be carried out. The EU is actively monitoring this area, as indicated by the plethora of legislative proposals underway or recently concluded. However, this abundance can actually cause confusion, as EU rules setting out specific rules for each offence category can make choosing the right instrument cumbersome. One of the key elements of the effective application of the instruments presented in the study is the institutional system, yet the EU legal acts presented have not managed to settle this issue satisfactorily. Although the EU rules enact instruments that can be used in criminal proceedings, they are not explicitly of a criminal law nature and allow Member States to confer powers on administrative authorities. The decisions and orders regulated or to be regulated have to be sent directly to service providers by the appointed authorities of the Member States, which will, as envisaged by the legislator, significantly accelerate collection of evidence. In Hungary, for example, the body competent to issue a removal order regulated in Decree 2021/784 is the Office of the

National Media and Infocommunications Authority pursuant to Section 12/B of the Act CVIII of 2001 on certain aspects of electronic commerce services and information society services.[28] A similar regulatory solution is expected to be adopted in Hungary pursuant to the DSA, as the National Media and Infocommunications Authority is expected play the role of digital service coordinator.

In the absence of proper coordination and communication, there is a likeliness of multiple bodies issueing multiple decisions calling for action on the same illegal content, ultimately reducing transparency and increasing the workload for both national authorities and service providers. With close inter-institutional coordination, these problems can be mitigated, but this only becomes measurable once the practical application has started.

References

Blaskó, B. & Budaházi, Á. (2019). *A nemzetközi bűnügyi együttműködés joga* [The law on international cooperation in criminal law enforcement]. Dialóg Campus.

Boros, A. (2016). *Közérthető közigazgatási hatósági eljárás* [Administrative procedures in an understandable way]. Wolters Kluwer Kft. eBooks. https://doi.org/10.55413/9789632956220

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime Law and Social Change, 46*(4–5), 189–206. https://doi.org/10.1007/s10611-007-9063-7

Brenner, S. W. & Koops, B-J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law, 4*(1), 786507. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507

Ligeti, K. (2008). A nemzetközi bűnügyi együttműködés általános feltételei [General conditions for international cooperation in criminal law]. In Kondorosi F. & Ligeti K. (Eds.), *Az európai büntetőjog kézikönyve* (pp. 60–75). Magyar Közlöny Lap- és Könyvkiadó.

Mezei, K. (2022). *A kiberbűnözés aktuális kihívásai a büntetőjogban* [Current challenges of cybercrime in criminal law]. L'Harmattan Kiadó, MTA Társadalomtudományi Kutatóközpont, Jogtudományi Intézet.

Parti, K. (2018). Az elektronikus hírközlési szolgáltatók együttműködési kötelezettsége a büntetőeljárás során a gyakorlat tükrében [The duty of cooperation of electronic communications service providers in criminal proceedings in the light of practice]. *Belügyi Szemle, 66*(10), 23–35. https://doi.org/10.38146/bsz.2018.10.2

Rawat, M. (2021). Transnational Cybercrime: Issue of Jurisdiction. *International Journal of Law Management & Humanities 4*(2). http://doi.one/10.1732/IJLMH.26049

Tóth, D. & Gáspár, Zs. (2020). Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén [Difficulties in international criminal cooperation related to cybercrime]. *Büntetőjogi Szemle,* 9(2), 35–45.

28 Act CVIII of 2001 on certain aspects of electronic commerce services and information society services.

Villányi, J. (2003). Az EU kölcsönös bűnügyi jogsegélyéről szóló egyezményhez kapcsolódó jogalkotási feladatok [Controlled delivery – the history and new possibilities for the methods against illegal trafficking]. *Acta Universitatis Szegediensis: Acta Juridica et Politica: Publicationes Doctorandorum Juridicorum III,* 209–259.

Online links in the article

URL1: *Least developed countries still lag behind in cyberlaw reforms*. https://unctad.org/news/least-developed-countries-still-lag-behind-cyberlaw-reforms

URL2: *Philippine Prosecutors Drop Charges in 'Love Bug' Case, WSJ*. https://www.wsj.com/articles/SB966862157148570125

URL3: *Ireland's Second Circuit Amicus Brief in Support of Microsoft*. https://www.eff.org/document/irelands-second-circuit-amicus-brief-support-microsoft

URL4: *Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence.*
https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf

Reference of the article according to APA regulation

Sorbán, K. (2024). Procedural dilemmas of cybercrimes involving illegal content dissemination in cross-border situations. *Belügyi Szemle*, *72*(1), 133–151. https://doi.org/10.38146/BSZ.2024.1.8