RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
November 16-17, 2023

DOI:10.5281/zenodo.10397848

EU-US Agreement on Combating Cybercrime

Simona Franguloiu[1], Nicoleta-Elena Hegheș[2]

[1]*Lecturer Contributor, PhD, Transilvania University Brașov, România,* simona.franguloiu@unitbv.ro*,*
Trainer at National Institute of Magistracy, Bucharest, Romania, simonafranguloiu@yahoo.com
[2] *Researcher 2nd Degree at "Andrei Rădulescu" Legal Research Institute of Romanian Academy, Bucharest, Romania, nicoleta.heghes@icj.ro; Professor, PhD, "Dimitrie Cantemir" Christian University of Bucharest, Romania, nicoleta.heghes@ucdc.ro*

ABSTRACT: Combating and preventing the commission of particularly serious offences, especially those related to cybercrime, requires a tailored response, which means making prevention work more effective, through the work of bodies and institutions with specific powers in this area, but also of judicial bodies that must cooperate, so that the existence of international instruments has become an absolute necessity. These are intended to strengthen international judicial cooperation (in addition to other activities) by coordinating efforts and actions to dismantle organized crime groups. Given the importance of electronic evidence in the investigation and prosecution of offenders in this area, in June 2019, the Council authorized the European Commission to start the procedure to start negotiating an agreement on behalf of the EU with the US on access to and collection of electronic evidence, negotiations which are ongoing. Of course, the subject matter of the agreement and the negotiated clauses are not public at the moment, but the European Commission regularly informs the Council on the state of these negotiations, so we intend to highlight the advantages of concluding this agreement as soon as possible from the perspective of international judicial cooperation.

KEYWORDS: cybercrime, EU-US agreement, international judicial cooperation, Budapest Convention, Second Additional Protocol, criminal investigation, electronic evidence, cross-border access

Introduction

It is fair to say that for many years, not only technological development, but in particular the information revolution, has changed and reformed the foundations of the entire society on all levels, starting with the economic, social, but above all, the informational. In recent years, digitization, which is used in all areas of activity, is turning into artificial intelligence, which is increasingly used.

The present scientific approach does not aim to analyze artificial intelligence, but only to take a sequential approach to the response that society offers to cross-border crime in this field. It is well known that both digitization and artificial intelligence have created new possibilities for malicious individuals to use new technologies to commit serious crimes such as terrorism, organized crime, trafficking in weapons, people, drugs, and the list is very long.

Combating and preventing the perpetration of particularly serious crimes requires a tailored response, which means making prevention work more effective, through the work of bodies and institutions with specific powers in this area, but also of the judicial bodies, which must cooperate, so that the existence of international instruments has become an absolute necessity. These are intended to strengthen international judicial cooperation (in addition to other activities) by coordinating efforts and actions to dismantle organized crime groups, as this study deals only with the judicial response, i.e. the identification of offenders, their investigation and prosecution, including trial work. At global and European level, there are several such instruments which we will not analyze, but we will mention the most important of them, namely the Budapest Convention on Cybercrime of 23 November 2001 (Council of Europe 2004, ETS No. 185, Treaty open for signature and ratification, entered into force on 1 July 2004).

Although this international act has so far been ratified by 68 states, it can be said that the instruments provided have proved to some extent to be insufficiently effective, given the significant increase in the number of crimes committed in this area of reference, and it is necessary to create instruments capable of eradicating this serious phenomenon. We believe that, first and foremost, given the speed with which not only information but also persons or goods intended for the commission of crimes are circulating, international judicial cooperation must be made more effective, so that the reaction of States is not only robust but also effective. This can only be achieved with a dynamic and speed at least equal to that of the criminals, all the more so as they disguise their illicit activity under the guise of legal or borderline legal activity.

1. Budapest Convention - Second Additional Protocol and its effects on international judicial cooperation

During the SARSCOV-2 pandemic, cybercrime increased exponentially, as many of the activities, where possible, took place online, which also led to a multiplication of the type and number of crimes committed, opening up new opportunities for organized crime groups. Most countries have therefore adopted different strategies in response to attacks by criminals on the most important social values protected by the criminal law. For example, Romania has adopted the National Strategy against Organized Crime (2021-2024), a document that offers "an integrated approach from an institutional and phenomenological point of view, with specific and individualized directions of action according to the legal competences of the institutions involved, with a focus on refining cooperation mechanisms in order to carry out actions to prevent and combat organized crime in a synergic manner". However, independently of the different strategies adopted by states, the most important document remains the Budapest Convention and its two Additional Protocols, in particular the Second Protocol on cybercrime and disclosure of electronic evidence.

As stated in the Preamble to the Protocol (European Commission 2022), cybercrime, cyber-attacks or ransomware attacks have grown exponentially and are increasingly specialized and complex, so that investigations cannot be carried out without close cooperation between judicial authorities, based on the principle of loyal cooperation, of course, and they urgently need the collection of evidence in electronic format, as these are cross-border crimes. Thus, the Proposal for a European Commission Decision authorizing the Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Budapest Convention on Cybercrime on enhanced cooperation and the collection of electronic evidence (European Commission 2022) which was opened for signature in May 2022.

The ratification of this Protocol marks a new stage in the approach to combating this type of crime, establishing not only enhanced forms of cooperation but also a new way of approaching international judicial cooperation through electronic evidence collection. To date (date of writing), the Protocol has been ratified by two States (Japan and Serbia) and has been signed without ratification by 40 States (Council of Europe 2023).

In essence, the European Union supports and sustains the implementation of this Convention in a coherent manner, not only through recommendations to Member States to ratify the Convention and the Second Additional Protocol, but also by funding working groups and capacity building programs. For example, the Recommendation for a Council Decision authorizing negotiations for a comprehensive international convention on combating the criminal misuse of information and communication technologies of 29 March 2022 (European Commission 2022) which will be the subject of a forthcoming scientific work by the authors.

The present study does not and cannot exhaust the subject of the Additional Protocol or the Convention within it, but only the relationship between this international document and the EU-US agreement on combating cybercrime.

It should be noted that, in essence, the Additional Protocol aims to bring about a substantial improvement in the area of international judicial cooperation by facilitating the obtaining and communication of electronic evidence between judicial actors, as it is currently held mainly by service providers in foreign jurisdictions. In the field of criminal justice, which is a feature of the rule of law, such evidence must be obtained and administered by the judicial bodies, which is in line with the principle of loyalty in the gathering and administration of evidence, as stressed in the preamble to the proposal for a decision.

The need has therefore arisen to use rules at international level, both substantive and procedural, to facilitate the international investigation and prosecution of persons who commit offences in this area, rules which are compatible at international level and which ensure that conflicts of law in the area of access to and transfer of electronic evidence are removed.

2. US-EU Agreement on cross-border access to electronic evidence

Given the importance of electronic evidence in the investigation and prosecution of offenders in this area, in June 2019, the Council authorized the European Commission to start the procedure for negotiating an agreement on behalf of the European Union with the USA on access to and collection of electronic evidence, negotiations which are ongoing (Council of Europe 2023b). Of course, the subject matter of the agreement and the negotiated clauses are not public at the moment, but the European Commission regularly informs the Council on the progress of these negotiations, so we intend to highlight the advantages of concluding this agreement as soon as possible.

One argument in favour of this agreement is that the negotiation of a new comprehensive international convention on combating the use of information and communication technologies for criminal purposes (ibid.) will take several years, given the possible reluctance of some states to relinquish their sovereign right to criminalize certain acts. We assert this because, as has often been pointed out in specialist doctrine, the law is the most characteristic expression of a state's sovereignty, and defining in such a comprehensive international act all the possible offences, as well as the procedural rules that should govern criminal investigation activity, the possible creation of and participation in joint investigation teams (although these exist and operate under the coordination of Eurojust, including with the participation of third states, and the USA has appointed a liaison prosecutor within the agency (EuroJust 2023a, 2023b) will make the negotiation procedure more difficult.

Consequently, we believe that the negotiation of the future comprehensive convention will take many years, and the subsequent procedure of signature, ratification, possible reservations, and declarations will take at least another 2-3 years.

Therefore, the conclusion of an agreement between the European Union and the USA would be easier and would have beneficial effects in terms of all phases of the criminal process (criminal prosecution, trial on the merits and appeals and enforcement of sentences, etc.) and we can estimate that the negotiation procedure itself could take less time, all the more so as these negotiations have already started in 2019.

From our point of view, this agreement should be based on the Budapest Convention and the provisions of the Second Additional Protocol, so that it can truly be an instrument that is not only practical and useful, but also compatible with existing international rules, precisely so that the latter do not remain devoid of practical effectiveness.

Most importantly, this future agreement should be efficient and effective in the work of law enforcement bodies. In this respect, we believe that a glossary of terms should be drawn up, first and foremost, in order to clarify certain criminal activities, precisely with a view to

ensuring that they are properly criminalized from the point of view of the unlawfulness and typicality of the acts. We support this assertion by arguing that these types of offences are committed using specific, highly technical technologies that are difficult to understand for people who are not trained in this field, such as lawyers, and for this reason we believe that these terms should be defined, with the proviso that this glossary should be able to be added to after the agreement has been concluded and adopted, as new technologies emerge, and that the list should not be exhaustive.

We also believe that, similarly to the Budapest Convention, it would be necessary to define offences in terms of the essential characteristic of the typical nature of the acts. The argument is that any criminal rule (which has a dichotomous structure in most legal systems) must clearly and explicitly state what the prohibited act of conduct is - verbum regens.

It should not be forgotten that the scope of cybercrime is wide, ranging from cybercrime as such to cybercrime committed by cyber means, such as online sexual exploitation of children, terrorist activities or other such crimes. In this regard, we believe that the exchange of information, opinions and opinions will prove to be of great value as an essential activity of judicial cooperation, since technologies will certainly evolve at an accelerated pace. Following this line of reasoning, it seems to us that it would also be useful and effective to set a limit (either minimum or maximum) on the applicable penalty, which would contribute to the predictability and predictability of the criminal law, which is an essential requirement of the principles of legality and criminality, principles known both in the legal systems of the Member States and in the USA.

Last but not least, we consider it necessary and useful to clarify certain forms of the offence, such as attempt, completed or completed offence, continuous or continued offence, as well as to establish the forms of criminal participation in their commission, i.e. instigation and complicity, and the conditions for the criminal liability of legal persons.

With regard to the rules of procedure, we believe that they should also follow the model already contained in the Budapest Convention and the Second Additional Protocol, which are designed to achieve the desired aim, namely combating cybercrime, while promoting the values and principles of the Union which correspond to those of the USA.

We refer, of course, to respect for the rights of suspects or accused persons in criminal investigations, respect for the fundamental principles of criminal proceedings - respect for the presumption of innocence, the right of defence, *non bis in idem,* fairness in obtaining and administering electronic evidence, and respect for and guarantee of all the procedural rights of the parties.

Conclusions

In view of the efficient way in which judicial cooperation relations between the USA and the Member States have been conducted so far, we believe that it would be useful to include provisions on the conditions to be met in the exercise of certain acts of criminal prosecution, such as computer searches, interception of accesses made, sometimes in real time, preservation of data stored on the accused person's computer and their transfer.

We also consider it necessary to have provisions on clear criteria for establishing jurisdiction for prosecution and trial, so as to avoid, as far as possible, conflicts of laws or jurisdictions. It is clearly necessary for the agreement to include provisions on how the judicial bodies will apply it in practice, given the effects and effectiveness of such an act from the perspective of public international law. In our view, a rethinking and repositioning of the powers and competences of the European Judicial Cybercrime Network (EJCN) (EuroJust 2023c) and, correlatively, those of Eurojust, as well as the practical use of specific channels for the communication of electronic evidence, should not be neglected. It is necessary to ensure that these types of critical infrastructure are perfectly secure so that they cannot

become accessible to criminals, given their major interest in escaping criminal liability. We are not yet in a position to say whether there is a need for provisions on victim assistance and protection, as there are multiple provisions in both EU and US law on this segment and we do not know the issues under negotiation, which are of a non-public nature.

Of course, we cannot replace the institutions and specialists who are carrying out the negotiations, but we can say that concluding this agreement as soon as possible would have beneficial effects in terms of combating cybercrime, because only criminals take advantage of the lack of these international acts, and when this agreement is concluded and applicable, it will reflect, to the highest degree, the moral aspect of the science of criminal law and criminal procedure.

References

Budapest Convention on Cybercrime of 23 November 2001, Treaty open for signature and ratification, entered into force 1 July 2004, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Council of Europe. 2004. Convention on Cybercrime (ETS No. 185). Available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Council of Europe. 2023a. "Chart of signatures and ratifications of Treaty 224." Available at https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224.

Council of Europe. 2023b. "Better access to e-evidence to fight crime." Available at https://www.consilium.europa.eu/ro/policies/e-evidence/.

EuroJust (European Union Agency for Criminal Justice Cooperation). 2023a. "Liaison Prosecutors." https://www.eurojust.europa.eu/states-and-partners/third-countries/liaison-prosecutors.

EuroJust (European Union Agency for Criminal Justice Cooperation). 2023b. "Joint investigation teams." Available at https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams.

EuroJust (European Union Agency for Criminal Justice Cooperation). 2023c. "European Judicial Cybercrime Network." Available at https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network.

European Commission. 2022. COM (2021) 719 final, 2021/0383(NLE) Proposal for a Council Decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Available at. https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52022PC0132&from=EN.

Proposal for a European Commission Decision authorizing Member States to ratify, in the interest of the European Union, the Second Protocol to the Budapest Convention on Cybercrime on enhanced cooperation and the collection of electronic evidence, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52021PC0719&qid=1699966238155.

Romania's National Strategy against Organized Crime 2021-2024, https://lege5.ro/App/Document/ha4dinjrg4yq/hotararea-nr-930-2021-privind-aprobarea-strategiei-nationale-impotriva-criminalitatii-organizate-2021-2024.

Second Additional Protocol to the Budapest Convention on Cybercrime and Disclosure of Electronic Evidence, https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52021PC0719&from=EN.