SARA Law Research Center
International Journal of Legal and Social Order, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
Nº. 1 (2026), pp. 1-9

PREVENTING AND COMBATING CYBERCRIME IN LIGHT OF THE REGULATIONS OF THE UNITED NATIONS CONVENTION AGAINST CYBERCRIME

A-C. MOISE

Received 05.03.2026; accepted 25.04.2026
First online publication: 27.04.2026
DOI: https://doi.org/10.55516/ijlso.v6i1.312

Adrian-Cristian MOISE
Professor, PhD, Habil.
Spiru Haret University, Faculty of Juridical, Economic and Administrative Sciences, Craiova
E-mail: adrian.moise@spiruharet.ro
ORCID ID: https://orcid.org/0000-0001-8755-0563

Abstract

Cybercrime is a rapidly evolving threat that affects national security, economies and individual rights. As the United Nations Convention on Cybercrime is the first international attempt to create a global legal framework against cybercrime, the article presents and analyzes aspects regarding the criminalization of new types of cybercrime, given the continuous development of information and communications technology. This article explores whether United Nations member states are prepared to face the practical and legal challenges of implementing this new global instrument. At the same time, the article highlights that digital evidence has gained increasing importance in the context of cross-border criminal investigations. Countries face difficulties in collecting digital evidence from transnational investigations and legal discrepancies.

Key words: *cybercrime, United Nations Convention, international cooperation, legal harmonization, digital evidence.*

INTRODUCTION

Cybercrime is a growing threat to the security of citizens and businesses in the European Union. According to a threat assessment conducted by Europol in the year of 2024, cybercrime has increased dramatically in terms of volume, intensity and potential for harm. At the same time, digital evidence has gained increasing importance in the context of criminal investigations. The United

Nations Convention against Cybercrime was adopted by the United Nations General Assembly in December 2024.

According to the Convention, the European Union and other regional economic integration organizations may sign and ratify the Convention, if at least one of its member states signs and ratifies it.

The United Nations Convention on Cybercrime will be open for signature on the 25th of October 2025, and will last until the 31st of December 2026. It shall enter into force ninety days after the deposit of the fortieth instrument of ratification, acceptance, approval or admission. In addition, the Presidency will give priority to finalising the appropriate Council decision for the European Union and its Member States to conclude the United Nations Convention on Cybercrime, with a view to seeking the consent of the European Parliament.

The United Nations Convention on Cybercrime is the first international attempt to create a global legal framework against cybercrime, while the Council of Europe Budapest Convention on Cybercrime was the established framework for cooperation in the field of cybercrime between members of the Council of Europe.

The United Nations Convention extends the scope to a wider range of crimes, provides universal access and technical cooperation mechanisms, but raises serious concerns about legal ambiguity, potential for surveillance and human rights safeguards.

Cybercrime is a rapidly evolving threat that affects national security, economies and individual rights. This study explores whether the United Nations states are prepared to face the practical and legal challenges of implementing this new global instrument.

Countries face difficulties in collecting evidence from transnational forensic investigations and legal discrepancies. The Council of the European Union adopted on the 13th of October 2025 a decision authorizing the European Commission and the Member States of the European Union to sign a United Nations Convention against Cybercrime. The United Nations Convention is an international treaty that establishes common rules worldwide to enhance cooperation in the field of cybercrime and the exchange of evidence in electronic format for the purpose of forensic investigations or criminal proceedings. IT fraud, large-scale hacking, child sexual abuse and online exploitation, as well as other forms of cybercrime are constantly on the rise.

By adopting this international legal instrument, an important step has been taken in the global fight against this type of crime, the crime that is committed in cyberspace.

PREVENTING AND COMBATING CYBERCRIME IN LIGHT OF THE REGULATIONS OF THE UNITED NATIONS CONVENTION AGAINST CYBERCRIME

I. LEGAL ASPECTS AND OBJECTIVES OF THE UNITED NATIONS CONVENTION AGAINST CYBERCRIME

One of the main objectives of the United Nations Convention agains Cybercrime concerns the criminalization of certain behaviours: mandatory criminalization of cybercrimes, for example, the unauthorized access to data or damage to the computer system, child exploitation, the use of Information and Communication Technology -ICT- for terrorist purposes. A key aspect of the United Nations Convention is the harmonisation of the criminalisation of certain cyber-related offences among participating countries. This means that all countries will take steps to include certain behaviours (for example, IT fraud or illegal interception) in their national legislation. The Convention will also give impetus to the criminalization of acts related to online child sexual abuse material, grooming and the dissemination of intimate images without consent. These crimes are already criminalized at European Union level, but not at a wider international level.

The most important crimes included in the United Nations Convention agains Cybercrime are the following *(United Nations Convention agains Cybercrime, 2024, pp. 5-8)*: crimes related to data and computer systems, such as, illegal access and illegal interception of an electronic communication, interference with an information and communications technology system, misuse of devices, information and communications technology system-related forgery and information and communications technology system-related theft or fraud; content-related offences, such as offences related to online child sexual abuse or child sexual exploitation material, solicitation or grooming for the purpose of committing a sexual offence against a child through an ICT system and the dissemination of intimate images without consent.

Regarding the crime of luring children for sexual purposes on the Internet, also known as online grooming, we would like to point out that this crime is included also in the Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse of children, the sexual exploitation of children and child pornography, which stipulates in Article 1 the following: "establishing minimum rules on the definition of criminal offences and sanctions in the areas of sexual abuse and sexual exploitation of children, child pornography and luring children for sexual purposes".

Article 6(1) of the Directive 2011/93/EU provides for the offence of solicitation of children for sexual purposes, which consists of "the proposal, made by means of information and communication technology, by an adult to meet a child who has not reached the age of sexual consent for the purpose of committing any of the offences set out in Article 3(4) (engaging in sexual activities with a child who has not reached the age of sexual consent) and Article 5(6) (producing

child pornography), where the proposal was followed by concrete acts establishing such a meeting, shall be punishable by a maximum term of imprisonment of at least one year" *(Directive 2011/93/EU, 2011, p. 8)*.

Also, in the content of Article 6 paragraph (2) of the Directive 2011/93/EU, the attempt made through information and communication technologies to commit the offences stipulated by the Article 5 paragraph (2) (acquisition or possession of child pornography) and by Article 5 paragraph (3) (knowingly obtaining, through information and communication technology, access to child pornography) by an adult who entices a child who has not reached the age of sexual consent to provide child pornography in which that child is depicted is criminalized *(Directive 2011/93/EU, 2011, p. 8)*.

The crime of luring children for sexual purposes, also known as grooming, is a crime often committed in cyberspace *(Davidson, 2011, pp. 8-26)*. Online grooming is also criminalized in other legal instruments, such as, for example, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, specifically in the Article 23 thereof. The Explanatory Report of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse at point 156 defines the notion of grooming, which refers to the preparation of a child for sexual abuse, motivated by the desire to use the child for sexual pleasure. This situation may involve befriending a child, often the perpetrator pretending to be a young person, engaging the child in discussing intimate matters and gradually exposing the child to sexually explicit material in order to reduce his sexual resistance or inhibitions *(The Explanatory Report of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 2007, p. 23)*.

At the same time, children can be drawn into the activity of producing child pornography by transmitting compromising personal photos via digital camera or webcam, providing the offender with a means of controlling the child through threats *(Bavisi; Graham; EC-Council, 2010, pp. 346-355)*. If a physical meeting is arranged, the child can be sexually abused or even injured *(Mattei Ferraro; Casey, 2005, pp. 101-149)*.

Other crimes included in the United Nations Convention agains Cybercrime are the following *(United Nations Convention agains Cybercrime, 2024, pp. 9-10)*: laundering of proceeds of crime; liability of legal persons; forms of participation and attempt in crimes. The United Nations Convention agains Cybercrime brings as novelties compared to other international and European legal instruments in the field of combating cybercrime, the regulation of the crime of money laundering through the Internet, as well as the liability of legal entities for committing cybercrimes *(Adeoyé, 2014, pp. 55-95)*.

All signatories to the United Nations Convention agains Cybercrime undertake to cooperate in investigating and prosecuting the crimes covered by the Convention. This includes collecting and sharing electronic evidence.

International cooperation applies to cybercrime, but also to serious crimes, such as international organized crime, if they are punishable by a prison sentence of at least four years.

The Convention promotes cross-border collaboration in the exchange of information, intelligence gathering, joint investigations and mutual legal assistance in cases of money laundering.

The procedural measures stipulated by the United Nations Convention against Cybercrime refer to the following: preservation; disclosure and production; search and seizure; real-time collection; freezing, distraint and confiscation of assets; Protection and assistance for victims and witnesses.

The forms of international cooperation sipulated by the United Nations Convention against Cybercrime refer to the following: extradition; mutual legal assistance; transfer of proceedings; joint investigations; confiscation and return of assets; mutual legal assistance for procedural measures.

The Convention supports the harmonization of national legislation on cybercrime and the misuse of ICTs to ensure legal consistency across jurisdictions.

Regarding respect for sovereignty, the United Nations Convention against Cybercrime emphasizes the principle of state sovereignty and non-interference in internal legal systems in the framework of international cooperation.

On the capacity to build mutual assistance, the Convention encourages support for developing countries for training infrastructure, legal reform and digital forensic investigation capabilities.

United Nations Convention against Cybercrime also lists some guarantees regarding human rights and data protection. The Convention recognizes the need to respect fundamental rights, including privacy, freedom of expression and procedural guarantees during the implementation of the treaty. The Convention comes with important safeguards to prevent abuse by participating countries to commit or legitimize human rights violations. Any interpretation that would lead to the suppression of human rights or fundamental freedoms, in particular freedom of expression, conscience, opinion, religion or belief, peaceful assembly and association, is explicitly excluded.

These safeguards also ensure that international cooperation can be refused, if countries believe it is being used to commit human rights violations or if requests are considered to be politically motivated.

The international cooperation may also be refused if such cooperation would be contrary to the domestic law of a country or if the refusal would be necessary to avoid any form of discrimination.

Ţhe United Nations Convention against Cybercrime establishes a global legal framework in the field of cybercrime, in the sense that this legal instrument

establishes a unified and binding legal framework for all signatories, with a view to effectively preventing, investigating and prosecuting cybercrime.

II. SOME CRITICAL VIEWS ON THE UNITED NATIONS CONVENTION AGAINST CYBERCRIME

However, this Convention also produces some obvious legal discrepancies.

First of all, we noticed that the Convention makes references to legal systems on a broad scale, civil law versus common law and authoritarian versus liberal systems.

Secondly, we noted that this Convention does not contain a universally accepted definition of cybercrime, for example, and of crimes that depend on cybernetics, crimes facilitated by cybernetics.

Thirdly, we have observed that national legal orders may conflict with or be incompatible with the standards of the Convention.

We can provide some examples of legal conflicts within Mutual Legal Assistance, such as:

- The European Union against Russia. The use of the 2016/679 General Data Protection Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, prohibits data transfers without adequate protection. Russia's 2015 Data Localization Law requires that Russian citizens' data be stored locally, therefore, cross-border sharing of digital evidence is legally blocked or delayed.
- The United States of America against China: The United States of America considers that all procedural guarantees should be respected and all the procedures in the criminal investigation must be carried out with judicial authorization. China criminalizes broad categories of crimes in disagreement with the principles of international criminal cooperation for obtaining digital evidence in the computer network. Mutual legal assistance is therefore hampered by the lack of trust and legal incompatibility.

These discrepancies may lead to inconsistent implementation of the Convention and weaken its effectiveness in real-time international criminal cooperation.

Another criticism we bring to the United Nations Convention against Cybercrime refers to the lack of legal procedures specific to cyberspace within this new legal instrument in the field of combating cybercrime.

Member States must provide for cyber-specific provisions on: a) preservation of data stored on a computer system b) preservation and disclosure of transmitted data c) provision of information d) investigation and seizure of stored data e) real-time collection of data in transit and f) monitoring of interception of data content.

The current procedural provision in the United Nations Convention against Cybercrime should be supplemented to improve the ability of judicial and police

authorities to conduct their investigations in real time, so as to collect the necessary digital evidence within the geographical limits of each national territory before this evidence is lost.

The cross-border nature of cybercrime requires the creation of a network of permanent contact points to facilitate the rapid processing of requests for assistance by member states of the United Nations Convention against Cybercrime.

The United Nations Convention against Cybercrime in its current regulatory form may generate broader political and legal conflicts.

Regarding jurisdictional conflicts, the legislators of the Convention should establish who/which judicial body investigates a cybercrime committed in several states, given that a network of contact points is stipulated at the level of the Council of Europe Convention on Cybercrime. Also, according to the provisions of the Convention, the principle of territorial sovereignty, although fundamental, can become a barrier to international criminal cooperation, necessary for the effective fight against cybercrime. At present, we believe that the lack of a common/uniform understanding of the rules for cross-border data access has created a significant obstacle to the international criminal cooperation in the field of cybercrime.

At the same time, it is possible that international criminal cooperation needed to combat cybercrime is affected by inconsistencies in the data protection legislation, such as the contrast between the General Data Protection Regulation - GDPR- and other weaker standards in the field of personal data protection.

The absence of secure and standardized mechanisms for cross-border computer data exchange creates significant challenges for international criminal cooperation in the field of cybercrime. Without clear rules, the law enforcement agencies face traditional legal obstacles when trying to access digital evidence held in other countries.

Currently, there are several challenges in terms of international criminal cooperation in the field of combating cybercrime: real-time cooperation and exchange of digital evidence remain idealistic for many countries; political tensions, for example, between the United States of America, China and Russia, could obstruct international criminal cooperation in the field of combating cybercrime; trust deficits persist, and countries may be reluctant to share sensitive computer data; mutual legal assistance treaties are often slow and bureaucratic.

Given the issues presented, we will address the following critical questions:

- Are states willing to adapt their domestic laws and institutions to combat cybercrime according to the United Nations Convention against Cybercrime?
- Can authoritarian regimes comply with human rights obligations?

o Will legal harmonization be pursued/achieved in good faith or manipulated for state control?

o Can technical implementation be fair/just between rich and poor states?

Such questions are not rhetorical. They concern crucial issues and areas, such as the rule of law and international politics and international law.

CONCLUSION

The United Nations Convention against Cybercrime represents a promising, but challenging step towards a global cyber governance. Without alignment, trust and capacity, its implementation at the international level is symbolic.

The successful application of this new legal instrument in the field of combating cybercrime will require: the broadest possible international participation; rights-based legal reforms; and a long-term international engagement of as many countries as possible. Member States need not only the capacity to transpose/implement the provisions of the Convention, but also political will and legal alignment based on international law of fundamental human rights and freedoms.

As future steps, the Convention legislators must: develop strategies for implementation, adapted to the needs of each region; encourage transparency, reporting and regular evaluation mechanisms; promote training and knowledge exchange between Member States; keep human rights and civil liberties at the heart of all efforts to combat cybercrime.

BIBLIOGRAFIE

1. Adeoyé Leslie Daniel (2014). *Legal Principles for Combatting Cyberlaundering*, Heidelberg: Springer International Publishing Switzerland;

2. Bavisi Sanjay; Graham Steven. EC-Council. Press (2010). *Computer Forensics. Investigating Network Intrusions and Cybercrime*, Clifton Park, New York: Cengage Learning;

3. Davidson Julia (2011). *Legislation and policy: protecting young people, sentencing and managing Internet sex offenders*, in Davidson Julia; Gottschalk Peter (eds.). *Internet Child Abuse. Current Research and Policy*, Abingdon, Oxon: Routledge, Taylor & Francis Group;

4. Mattei Ferraro Monique, Casey Eoghan (2005). *Investigating Child Exploitation and Pornography: The Internet, The Law and Forensic Science*, Burlington, Massachusetts: Elsevier Academic Press;

5. United Nations, General Assembly, *United Nations Convention agains Cybercrime*, 7 August 2024;

6. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of

children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Official Journal of the European Union, L 335/1, 17.12.2011;
7. Council of Europe Treaty Series- No. 201*, Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* , Lanzarote, 25.X.2007.