Publicationes Universitatis Miskolcinensis
Sectio Juridica et Politica, Tomus XLIII/2 (2025), pp. 220–248.
https://doi.org/10.32978/sjp.2025.025

CYBER AGGRESSION CRIMES: A COMPARATIVE STUDY OF THE JORDANIAN AND THE HUNGARIAN LEGAL FRAMEWORKS

A kiberagresszióval kapcsolatos bűncselekmények: a jordániai és a magyar jogi keretek összehasonlító vizsgálata

FERENC SÁNTHA* – HUTHAIFA ALBUSTANJI**

The rapid advancement of the Internet and information and communication technologies in the 21st century has reshaped criminal activities, introducing new challenges for legal systems worldwide. Governments face increasing pressure to develop cyber laws that effectively support law enforcement in combating cybercrime. Among these challenges, cyber aggression has emerged as a significant concern, particularly in Jordan and Hungary, where legal frameworks have undergone modifications to address evolving threats. This study provides a comparative analysis of the legal approaches to cyber aggression in both countries, examining the effectiveness of their implementation and enforcement in practice

Keywords: *cyber aggression crimes, disinformation, hate speech, false news, cybercrimes, Jordan, Hungary*

Az internet, valamint az információs és kommunikációs technológiák gyors fejlődése a 21. században átformálta a bűnözést, és világszerte új kihívások elé állította a jogrendszereket. A kormányokra egyre nagyobb nyomás nehezedik, hogy olyan kiberjogszabályokat dolgozzanak ki, amelyek hatékonyan támogatják a bűnüldözést a kiberbűncselekmények elleni küzdelemben. E kihívások közül a kiberagresszió jelentős aggodalomra ad okot, különösen Jordániában és Magyarországon, ahol a jogi kereteket az újabb fenyegetések kezelése érdekében módosították. A tanulmány összehasonlító elemzést nyújt a két ország kiberagresszióval kapcsolatos jogi megközelítéseiről, megvizsgálva azok gyakorlati végrehajtásának és érvényesítésének hatékonyságát.

* FERENC SÁNTHA
associate professor
University of Miskolc
Faculty of Law
Department of Criminal Law
3515 Miskolc-Egyetemváros
ferenc.santha@uni-miskolc.hu

** HUTHAIFA ALBUSTANJI
Ph.D Student
University of Miskolc
Faculty of Law
Deák Ferenc Doctoral School
Bustanjiii@yahoo.com

Kulcsszavak: *kiberagresszióval kapcsolatos bűncselekmények, dezinformáció, gyűlöletbeszéd, álhírek, kiberbűncselekmények, Jordánia, Magyarország*

Introduction

In the digital era, the internet and technology have become integral to daily life, transforming how we communicate, work, and interact.[1] While these advancements offer numerous benefits, they have also led to new forms of online misconduct, including cyber aggression crimes. These offenses involve deliberate harmful actions against individuals or entities, such as publishing hate speech on social media, spreading false information on the internet, and engaging in Cyber defamation or the character assassination of public figures, all of which can have significant psychological, social, and legal consequences. Therefore, it is essential to examine how different countries address these crimes to evaluate the effectiveness of their legal frameworks.

This paper aims to make a comparative analysis of the newly introduced legal rules on cyber aggression crimes in Jordan and Hungary. These regulations have faced significant criticism from scholars, as they limit freedom of expression in cyberspace in both countries. Therefore, a deeper understanding of their enforcement mechanisms is essential to ensure their implementation is not left to broad interpretations by public entities like the police and public prosecution departments. Based on these concerns, the main question this paper seeks to answer is: To what extent do the new cyber aggression laws in Jordan and Hungary balance cyber freedom with the protection of individuals in cyberspace?

The importance of this study stems from the fact that cyber aggression can affect anyone using social media or other online platforms that publish content for public interest, such as journalism. Considering that the previous cyber aggression rules were less restrictive on cyber freedom yet still faced objections, the introduction of stricter regulations has sparked significant debate by most internet users in both countries regarding the reasons behind their enactment and their implementation. Therefore, the first chapter will provide a general insight into cyber aggression crimes, the second chapter will conduct an in-depth analysis of Jordan's cyber aggression crimes, and the third chapter will examine the Hungarian perspective on these crimes.

1. The evolution of cybercrime: understanding the rise of cyber aggression

There is no doubt that the use of technologies has created a cyberspace that allows individuals to commit criminal activities from anywhere in the world, all while seated at home in front of their personal computer connected to the Internet. These activities are becoming a significant threat to individuals, companies, and governments. One of these activities is cyber aggression.

---

[1] Abhilash CHAKRABORTY – Anupam BISWAS – Ajoy Kumar KHAN: *Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation*. arXiv, 27 September 2022, https://arxiv.org/abs/2209.13454, 4 March 2025.

Cyber aggression is defined as the intentional use of electronic means to harm, harass, or manipulate others online, including behaviors such as spreading rumors, sending offensive messages, hacking personal data, and impersonation.[2] The term cyber aggression is partially similar to cyberbullying, which refers to the repeated use of digital technology to harass, intimidate, or harm someone, typically among children or teenagers.[3] However, cyber aggression is a broader term that does not necessarily require repeated actions. Despite this distinction, both cyber aggression and cyberbullying share similarities, as they are crimes committed within cyberspace. Finally, terms 'harassment in cyberspace' and 'stalking' are also known in the literature, but these are also narrower categories than cyber aggression.[4]

To this extent, social media has become a key platform for cyber aggression. While it provides innovative ways to communicate and connect with peers both nationally and globally, it has also expanded forms of cyber aggression that exist solely in the online realm, such as cyber hate speech, character assassination, and cyberstalking.[5]

As a result of the spread of these cyber activities, many states have responded by enacting cybercrime laws to combat cyber threats, including cyber aggression. For instance, the EU Digital Services Act (DSA) 2022 provides comprehensive regulations to tackle harmful online content and holds platforms accountable for cyber aggression.[6] Additionally, Jordan's Cybercrime Law No. 19 of 2023 addresses various forms of cybercrime, including cyber aggression and harassment.[7] Similarly, the Hungarian Criminal Code (Act C of 2012) outlines criminal offenses related to cyber aggression and online harassment, ensuring legal protection against such activities in Hungary.[8]

---

2 Muhammad Kamal UDDIN – Jakia RAHMAN: Cyber Victimization and Cyber Aggression among High School Students: Emotion Regulation as a Moderator. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 16/2., April 14, 2022, 2. https://doi.org/10.5817/CP2022-2-4

3 Ju BINJI: Impacts of Cyberbullying and Its Solutions. Lecture Notes in Education Psychology and Public Media 29 (December 7, 2023), 254. *Proceedings of the 2nd International Conference on Interdisciplinary Humanities and Communication Studies*. https://doi.org/10.54254/2753-7048/29/20231521

4 According to Clough, stalking may be described as 'a course of conduct in which one individual inflicts on another repeated unwanted intrusions and communications, to such an extent that the victim fears for his or her safety'. Jonathan CLOUGH: *Principles of cybercrime*. Cambridge, 2010, 365.

5 Jillian K. PETERSON – James DENSLEY: Cyber violence: What do we know and where do we go from here? *College of Liberal Arts All Faculty Scholarship* (2017), 5:9. https://digitalcommons.hamline.edu/cla_faculty/5, 4 March 2025.

6 European Union, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 December 2022 on a Single Market for Digital Services (Digital Services Act). *Official Journal of the European Union* L 333, 27 December 2022, 1–75.

7 Electronic Crimes law No. 17 of 2023, *Official Gazette* 5874, 3579. Dated 13-08-2023.

8 Hungary, Criminal Code (Act C of 2012 on the Criminal Code), *Hungarian Official Journal*, 2012, available at: https://net.jogtar.hu/jogszabaly?docid=A1200105.TV.

When discussing cyberaggression, it's important to understand its different types in relation to other cybercrimes, as cybercrimes manifest in various forms. Some of these crimes directly impact individuals by violating ethical principles like respect, empathy, and personal integrity, deeply influencing the morality of those involved, such as in cyber aggression offenses. Other crimes focus on attacking individuals' data, often for blackmail or to steal information for different purposes, which can be considered a more indirect form of cyber aggression. In these cases, the main objective isn't direct personal confrontation or emotional harm in real-time, but rather a more covert or strategic approach. Additionally, another category of cybercrime targets networks and information systems, impacting assets owned by individuals, companies, or governments. These offenses are typically not classified as cyber aggression, as they focus on the system itself, aiming to disrupt, steal, or manipulate data, often driven by financial, strategic, or political motives.

Cyber aggression involves hostile actions or behaviors that utilize technology, particularly the internet, to cause harm, disrupt, or intimidate individuals, groups, or organizations. Consequently, spreading false information or news to damage a government's reputation falls within the scope of cyber aggression. Given the rapid rise of these activities, it's essential to consider the severe impact they have on both individuals and society as a whole.

Cyber aggression has negatively impacted various sectors of society, causing significant harm to a country's economic and social development. The long-term effects of cyber aggression extend beyond emotional and psychological distress, leading to physical health issues and negative social consequences. Victims often experience physical impacts, such as psychosomatic disorders, including sleep problems, headaches, abdominal pain, anorexia, and nausea, which may lead to reduced concentration and worse academic or work performance.[9]

Additionally, emotional impacts are severe, with victims experiencing anxiety, loneliness, depression, mood swings, and fear, particularly regarding their safety. These emotional consequences can persist long-term, exacerbating the initial harm. Consequently, cyber aggression not only affects individuals but also undermines productivity and social well-being, having far-reaching effects on both the personal and societal levels.[10]

Due to the numerous impacts of cyber aggression, it is essential for states to proactively address and stay ahead of this growing threat by proactively developing effective strategies to counter such risks and prevent their occurrence. These strategies should be based on a comprehensive legislative framework that operates at both national and international levels. A balance must be struck between

---

[9] Kamil KOPECKY – René SZOTKOWSKI: Cyberbullying, Cyber Aggression and Their Impact on the Victim – The Teacher. *Telematics and Informatics* 34/2., May 2017, 506–517. https://doi.org/10.1016/j.tele.2016.08.014

[10] J. M. JENKINS – K. OATLE: Psychopathology and short-term emotion: the balance of affects. *Journal of Child Psychology and Psychiatry, and Allied Disciplines* 41/4., 2000, 463–472. https://doi.org/10.1017/S0021963000005709

safeguarding individual freedoms in cyberspace and taking into consideration the national security needs of the state. The following chapters will explore this issue in the contexts of Jordan and Hungary.

2. Cyber aggression crimes under Jordanian legal system

2.1. Historical development of cyber aggression crimes in Jordan

The concept of cyber aggression was not officially recognized in Jordanian law for a long time, even as cybercrimes became more common in the early 21st century.[11] In 2010, Jordanian authorities took the initiative to lead regional efforts in drafting a convention aimed at combating cyber-related crimes in Arab countries. This convention provided a framework for criminalizing cyber aggression at both national and regional levels. These efforts resulted in the adoption of the Arab Convention on Combating Information Technology Crimes on December 12, 2010, which officially came into effect on June 17, 2012.[12]

Accordingly, in 2010, Jordan introduced its first cybercrime law, Temporary Information Systems Crime Law No. 30 of 2010, marking a significant step toward criminalizing cybercrimes at the national level.[13] However, the law initially addressed cyber aggression in a limited scope, focusing on offenses such as the dissemination of pornographic content, online blackmail and sexual exploitation of minors, promotion of prostitution, and the use of information systems or networks for terrorist activities, including incitement to violence against individuals or communities.[14]

Despite this gradual approach to addressing cyber aggression, the law eventually expanded to include a wider range of offenses, such as cyber defamation, cyber hate speech, and character assassination through online platforms. This limited initial focus may be attributed to the relatively low popularity of social media applications at the time. Since most internet users engaged with websites rather than interactive communication platforms, the prevalence of crimes like cyber defamation and online hate speech was not as pronounced as it would later become.

Subsequently, in June 2015, Jordan enacted a new cybercrimes law called the Electronic Crimes Law No. 27 of 2015,[15] which replaced Temporary Information Systems Crime Law. The Electronic Crimes Law introduced new forms of cyber

---

[11] Ashish Kumar, SRIVASTAVA – Rakesh Kumar, SINGH: Legal Control of Right to Speech and Expression in Virtual Space. In: *Cyber Crimes in 21st Century.* Manakin Press Pvt. Ltd., 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4652034, 4 March 2025.

[12]. League of Arab States. *Arab Convention on Combating Information Technology Crime*. (2010). https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf, 4 March 2025.

[13] Temporary information systems crime law No. 30 OF 2010.: *Official Gazette* 5056, Jordan, p. 5334, dated 16-09-2010.

[14] Ibid., Art. 8, 9, and 10.

[15] Electronic crimes law No. 27 OF 2015: *Official Gazette* 5343, Jordan, 5631, dated 01-06-2015.

aggression crimes like Defamation, Insult, and Contempt Crimes which involved any online publications that involve these practices.[16]

In 2023, Jordanian authorities enacted a new cybercrimes law to expand the scope of criminalized cyberattacks. On September 12, 2023, after completing the legislative process, the law was officially coming into force.[17] However, it sparked significant debate among Jordanian citizens as it introduced new categories of cyber aggression crimes, including cyber hate speech, publications for false news, online character assassination, and cyber fraud.

2.2. Ambiguities in new cyber aggression crimes concepts

While the historical development of cyber aggression laws in Jordan has been marked by significant steps, a new challenge has emerged with the introduction of unclear and ambiguous terms in the 2015 and 2023 electronic crimes laws, creating a potential for inconsistent enforcement. To this extent, the controversy surrounding cyber defamation crimes provisions in both laws were criticized for imposing heavy sanctions. Many viewed these penalties as a restriction on freedom of expression in cyberspace. Art. 11 of the previous law in conjunction with Art. 16 of the new law was not directly related to online publishing, but it applied to all forms of publishing and republishing on the Internet, whether on public or private platforms. This approach contradicted the general principles outlined in the Jordanian criminal code, which typically requires publicity as a key condition for establishing the legal grounds for most defamation crimes.[18]

A study conducted by scholar Sakher Ahmad Al-Khasawneh revealed that, in his personal opinion, the Jordanian cybercrime law guarantees freedom of information at a theoretical level, but in practice, it only achieves about 65% effectiveness. The study also identifies a clear imbalance in the Electronic Crimes Law, which appears to conflict with journalists' right to criticize. It recommends that Art. 11 of the Cybercrime Law be amended to remove all restrictions on publishing content online.[19]

Building on the legal framework discussed earlier, we now turn to explore how these ambiguities manifest in specific cyber aggression crimes, such as cyber hate speech and false news, and character assassination which have become more prevalent in recent years. These crimes were introduced in the electronic crime Law No. 17 of 2023.

---

[16] Ibid, Art. 11 which states 'Whoever intentionally sends, resends, or publishes data or information through the information network, the website, or any information system that involves defamation, Contempt, or insulting anyone, shall be punished with imprisonment for a period of no less than three months and a fine no less than (100) one hundred dinars and it does not exceed (2000) two thousand dinars'.

[17] Electronic Crimes Law No. 17 Of 2023.

[18] Art. 189 of the Jordanian Penal Code No. 16 of 1960 and Its Amendments, *Official Gazette*, No. 1487, Jordan, 374. Dated 1/5/1960.

[19] Sakher AL-KHASAWNEH: Effect of Article 11 of the Jordanian Electronic Crimes Law on Exercising Criticism Freedom for Journalists and Workers in the Digital Media. *Journal of Law, Policy and Globalization* 85, 2019, 48–61. https://doi.org/10.7176/JLPG

2.3. Cyber hate speech crimes

Over the past two decades, hate speech and hate crimes have increased significantly worldwide. This rise has been linked to factors such as growing concerns over migration and a series of economic and social crises. In 2019, during the launch of the United Nations Strategy and Plan of Action on Hate Speech, UN Secretary-General António Guterres highlighted disturbing global trends, including rising xenophobia, racism, intolerance, violent misogyny, antisemitism, and anti-Muslim sentiment.[20] As part of the digital world, Jordan has not been immune to this phenomenon and continues to grapple with online hate speech crimes.

The Cybercrime Unit at the National Security Department announced that cybercrimes in Jordan have increased sixfold since 2015, rising from 2,305 cases in 2015 to 16,027 cases in 2022. This surge is attributed to the widespread use of technology, digital applications, and social media, as well as increased public awareness of legal rights and the ability to file complaints. Among these crimes, 113 cases were related to hate speech and incitement, with authorities taking action against some offenders.[21]

The increase in cybercrime statistics in Jordan sounds the alarm for the Jordanian society, a study conducted by the researcher Naser Alrahamneh on Hate Speech on Facebook in Jordan found that Facebook plays a role in inciting discord among different segments of society, leading to division and conflict. The results also indicated that such platforms contribute to weakening social cohesion, making society more vulnerable during crises. The study also finds that hate speech on Facebook negatively impacts Jordanian religious, social, and cultural values. The results indicate that such discourse can lead to religious and sectarian extremism and conflict while also weakening social solidarity among people.[22]

In response to the growing impact of online hate speech, Jordan introduced a new article in Electronic Crime Law No. 17 of 2023 to criminalize such offenses. Under this law, anyone who deliberately uses digital platforms to urging hate speech, fuel division, threaten social peace, justify violence, or show contempt for religions faces 1 to 3 years in prison and/or a fine between 5,000 and 20,000 Dinars. While online hate speech has become a widespread issue, criminalizing it without clearly defining what constitutes incitement raises concerns. Broad interpretations could risk restricting freedom of expression, as even criticism of public officials might be misclassified as inciting hate crimes.[23] However, the lack of a clear definition of hate speech crimes may create ambiguity and inconsistency in how the law is applied, making it a

---

[20] *United Nations Strategy and Plan of Action on Hate Speech.* United Nations, https://www.un.org/en/genocide-prevention/hate-speech/strategy-plan-action, 4 March 2025.

[21] The Cybercrime Unit of the Public Security publishes its annual statistics for the year *2022*. *Public Security Directorate*, 2022. https://bit.ly/41CKHSB, 4 March 2025.

[22] Naser ALRAHAMNEH: *Hate Speech in Facebook in Jordan: Survey Study.* Middle East University, Jordan, 2018. https://meu.edu.jo/libraryTheses/5ca8335e8883e_1.pdf, 4 March 2025.

[23] Art. 17 of the Jordanian electronic crimes law No.17 of 2023

contentious issue that will continue to spark debate and scrutiny.[24] This opens the door to ask what consists hate speech in jurisprudence and international context.

According to the United Nations strategy and plan of action on hate speech, hate crimes are defined as "any kind of communication in speech, writing or behavior, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, color, descent, gender or other identity factor".[25] Jurisprudence categorizes hate speech into four main types, each targeting different aspects of society. The first is religious hate speech, which uses inflammatory language to provoke hatred and violence based on religious affiliation. The second type is racist hate speech, which involves discriminatory comments and actions against individuals based on their race or ethnicity. The third category is political hate speech, which arises during events like elections and referendums, where opposing views often lead to the spread of intolerance and hostility online. Finally, gendered hate speech targets individuals based on their gender or sexual orientation, frequently leading to online harassment and abuse.[26]

When examining the Jordanian legal provision addressing online hate speech, it's evident that the law integrates hate speech with other offenses, such as inciting division, threatening social peace, justifying violence, and showing contempt for religions. This integration overlooks the fact that these offenses should be considered as part of the broader category of hate crimes according to the definition of hate speech crimes internationally.

Furthermore, the legislator used term "Urging hatred" as indicator to online hate speech crime. However, the term "urging" is more commonly associated with encouraging positive or beneficial actions, which is incompatible with the intent of criminalizing hate speech. It is clear that the legislator may have intended to use the term "incitement" instead. Even so, "incitement" may not be the best fit for the crime itself, as the focus should be on criminalizing the act of online hate speech directly. The issue of incitement would then relate to the sanctions to be applied, as specified in Art. 80/1 of the Jordanian Penal Law.[27]

---

[24] Alaeldin Mansour MAGHAIREH: Cybercrime Laws in Jordan and Freedom of Expression: A Critical Examination of the Electronic Crimes Act 2023. *International Journal of Cyber Criminology* 18/1., 2024, 15–36.

[25] *United Nations Strategy and Plan of Action on Hate Speech (May 2019)*. United Nations https://www.un.org/en/genocide-prevention/hate-speech/strategy-plan-action, 4 March 2025.

[26] Sergio Andrés CASTANO – Natalia Suarez, BETANCUR – Luz Magnolia Tilano VEGA – Harvey MAURICIO – Herrera LOPEZ: Internet, Social Media and Online Hate Speech. Systematic Review. *Aggression and Violent Behavior* 58, 2021. https://doi.org/10.1016/j.avb.2021.101608

[27] Art. 81/1 of the Jordanian Penal code No. 16 of 1960 and Its Amendments states "a. A person who incites or attempts to compel another person to commit a crime by giving him money, giving a gift to him, or by influencing him by threat, trick, and deception, or by exploiting influence or misuse of the job judgment, is considered an instigator."

2.4. Publishing or republishing false news

The Jordanian Electronic Crimes Law No.17 for 2023 introduced publishing false news crimes as a new type of cyber aggressions crimes. Art. 15 of the stated 'Any person who willfully sends resends or disseminates data or information through the computer network information technology information system website or social media platform that includes false news targeting national security and community peace or libel slander or humiliation of any person shall be punished Imprisonment for a period of not less than three months or a fine of not less than (5000) five thousand Dinars and not exceeding (20000) twenty thousand Dinars or with both penalties'.[28]

Similarly, to hate speech crimes, the law does not provide a clear definition of false news, leaving its interpretation up to the judiciary. This could create inconsistencies, as what one judge considers false news may not be viewed the same way by another. The law also states that false news must target national security and community peace to be criminalized. However, these terms are vague and lack precision, making the law open to varied interpretations as well.

However, false news refers to information or stories that are not true, whether intentionally or unintentionally.[29] While fake news typically refers to deliberately fabricated or misleading stories created to deceive or manipulate the public.[30] The legislation does not criminalize the unintentional publication of false news, so the correct term to use would be the publication or republication of fake news intentionally targeting national security or social peace. In this regard, it is surprising that the right term "Publishing Fake News" is used correctly in the Art. 21 of the same law for online requesting gift or benefit crime, contrary to what is ruled in this article.[31] However, the article does not classify the creation of false news as a punishable offense, instead focusing solely on its transmission and publication.[32]

The Amman Magistrate's Court, in case No. 19411/2023, examined the application of Art. 15 of the Jordanian Electronic Crimes Law regarding the publication of false news. The case involved two defendants, both drivers for a smart transportation app, who shared a voice message and a written message via WhatsApp within a private group for drivers. The messages falsely claimed that a 5.6-magnitude earthquake would strike the Dead Sea region the following day, affecting an area of 50 km and reaching the governorates of Madaba and Balqa. They also warned of

---

[28] Art. 15 of the Jordanian Electronic Law No.17 of 2023.

[29] DON FALLIS: What Is Disinformation? *Library Trends* 63, 2015, 401–426, https://api.semanticscholar.org/CorpusID:13178809, 4 March 2025.

[30] E. C. TANDOC, Z. W. LIM, & R. LING., Defining "Fake News": A Typology of Scholarly Definitions. *Digital Journalism* 6, 2018, 137–153. https://doi.org/10.1080/21670811.2017.1360143

[31] Art. 21 of the Jordanian Electronic Law No. 17 of 2023.

[32] MAGHAIREH: *Cybercrime Laws in Jordan.* 2024, 15–36.

possible disruptions to internet services, phone networks, and other communication channels, urging people to take precautions.[33]

After reviewing the case, the court found that the concept of social peace refers to a state of harmony and stability within society, while national security involves the use of various means to ensure the proper functioning of all components of society, free from crises and rumors that could threaten public safety and the false message sent by the driver has target both social peace and national security. The court justified its decision stating that both concepts are subject to the discretion of the trial judge, who evaluates them based on the content of the published statements, as well as the time and place of their dissemination. In sum, the found the defendants guilty of publishing false news and issued its decision to convict them, imposing a fine of 5,000 dinars plus fees—the minimum penalty.[34]

It is clear that the court interpreted these concepts in an overly broad manner, as it did not establish that the intention behind sharing false news within a private WhatsApp group among friends or colleagues was to threaten national security. The court also failed to consider that the practice of forwarding unverified information is a common cultural norm in Jordan. Given the circumstances of the case, the decision, with all due respect, appears to be flawed. The primary issue stems from legislative shortcomings, as there is no clear legal definition of false news, social peace, or national security, leaving these terms open to broad and inconsistent judicial interpretation.

2.5. Cyber character assassination

Although cyber aggression crimes can target both individuals and organizations, as previously mentioned, cyber character assassination can only target individuals. This is because character is a personal concept, and only individuals possess a personal character. The Jordanian Electronic Crimes Law No. 17 of 2023 introduced cyber character assassination as a new form of cyber aggression.[35] However, like other recent cybercrimes, the concept of cyber character assassination remains debatable due to the lack of a clear definition of the term.

Jurisprudence defines it as the deliberate and continuous effort to damage the reputation of an individual by spreading false accusations, rumors, and manipulating

---

[33] Case No. 19411/2023, Amman Magistrate's Court, Judgment of 22 October 2023. *Amman Magistrate Court Databases*. https://petra.gov.jo/Include/InnerPage.jsp?ID=260623&lang=ar&name=news, 4 March 2025.

[34] Ibid.

[35] Art. 16 of the Jordanian Electronic Crime Law No.17 of 2023 states "Anyone who unjustly spreads, attributes, or attributes intentionally to a person or contributes to that via the information network, information technology, information system, or website or social media platforms, acts that would assassinate his personality shall be punished by imprisonment for a period of not less than three months or by a fine of not less than 5,000 five thousand dinars and not exceeding 20,000 twenty thousand dinars, or by both of these penalties."

information, with the goal of undermining that person's credibility and social standing.[36] The definition of the crime suggests that the targeted individual must have a reputation, and the actions of the perpetrators are aimed at damaging this reputation or social life.

However, it is noteworthy that the Jordanian legislator does not specify any particular characteristics, social, or political status of the person targeted for character assassination, meaning that anyone could be a victim of this crime. This overly broad approach may undermine the rationale for criminalizing cyber character assassination, which typically targets individuals with public visibility, controversial opinions, or vulnerable positions, such as public figures, activists, or marginalized groups.[37]

Unlike other cyber aggression crimes, which require the publication or republication of posts, images, sounds, etc., that lead to hate speech, false news, or defamation, the crime of cyber character assassination only necessitates the intentional spreading of false rumors or falsely attributing actions to someone via cyber means in order to damage their reputation. This broad definition opens the door for accusing individuals based on their online speech about any public figure, which contradicts basic standards of freedom of expression as protected by the Jordanian constitution, which guarantees the right to express opinions through all means.[38]

2.6. Special criminal measures for combating cyber aggression crimes in Jordan

Because cybercrimes, including cyber aggression, evolve alongside rapid technological advancements, it is essential to have procedural measures in place alongside legal sanctions.[39] Simply punishing offenders is not enough—without judicial orders to remove harmful content, such as hate speech posts, they can continue to be republished, undermining the effectiveness of sanctions. Accordingly, the Jordanian Electronic Crimes Law No. 17 of 2023 introduced Art. 31, which outlines a range of judicial measures specifically designed to combat cybercrimes and prevent their recurrence by others. In addition to the legal sanctions imposed on offenders, these measures grant the national courts the authority to take decisive actions, including confiscating devices and tools used in cybercrimes, blocking or

---

[36] Muntaser, ALQUDAH – Ahmad, AL-AMAWI – Tawfiq, KHASHASHNEH – Hashem, BALAS: The Crime of Character Assassination in the Jordanian Cybercrime Law. *International Journal of Religion* 5/10., July 11, 2024, 3671–3684. https://doi.org/10.61707/gsfk2s22

[37] Barjes Khalil Ahmad, AL-SHAWABKEH: Criminalization of Personality Assassination via Electronic Means. *Journal of Law and Sustainable Development* 12/1., 2024, 1–20.

[38] Art. 16 of The Constitution of the Hashemite Kingdom of Jordan, published in Official Gazette Issue No. 1093, 3, January 8, 1952, effective January 8, 1952. Amended multiple times, including 1954, 1955, 1958, 1960, 1965, 1973, 1974, 1976, 1984, 2011, 2014, 2016, and 2022. Most recent amendment: Issue No. 5770, 1139, January 31, 2022, effective January 31, 2022.

[39] Ibrahim Mohammad, ALRAMAMNEH – Amal, ABUANZEH: International and National Procedural Framework for Combating Cybercrime. *International Journal of Cyber Criminology* 17/2., July–December 2023, 333.

disabling websites, deleting unlawful data, and shutting down premises involved in illegal activities. Furthermore, the law criminalizes any obstruction of these measures, reinforcing the state's commitment to addressing cyber threats effectively.[40]

Although these measures are effective for non-spreading cyber aggression practices, but it contains many flaws. For instance, it allows the court to confiscate devices, programs, tools, and materials used in cybercrimes. However, it does not clearly define the criteria for what can be confiscated. Without clear guidelines, this broad discretion could lead to overly harsh penalties and the unjust seizure of property, potentially harming innocent third parties who had no involvement in the crime.

The procedural provisions on confiscation in Art. 31 of the Jordanian Electronic Crime Law, when compared with Art. 44 of the Jordanian Penal Code, reveal two key limitations. While Art. 44 of the Penal Code imposes restrictions on confiscation, Art. 31 does not. The two main limitations are: first, the need to consider the rights of third parties acting in good faith, and second, that confiscation should be limited to what is necessary for compensation purposes.[41] If applied to cybercrime cases, these restrictions will help strike a balance in confiscation decisions.

Additionally, as such as confiscation decisions, the suspension, disabling, or blocking of websites and information systems raise concerns about freedom of expression and access to information. As there is no specify clear criteria for imposing such measures, which could lead to potential misuse for political reasons.

The provision requiring the deletion of information or data at the offender's expense is problematic due to its lack of specificity regarding the type of information or data to be deleted. The article does not define what constitutes the "information or data" in question, leaving the decision to the discretion of the court. This ambiguity could lead to the deletion of data that is not directly relevant to the crime or even the removal of legitimate content, potentially infringing upon freedom of expression.

Furthermore, the provision does not account for the practical difficulties that may arise in holding offenders accountable for costs if they are located in a foreign jurisdiction. In cases of cross-border cybercrimes, it is often challenging to enforce

---

[40] Art. 31 of the Jordanian Electronic Crimes Law No. 17 of 2023 stats 'without prejudice to the rights of bona fide third parties In case of conviction the court shall decide on its own that: 1- Confiscate the devices programs tools tools means or materials used in the commission of any of the crimes stipulated in this Law or the funds derived therefrom 2- Suspending disabling or blocking the operation of any information system or website used in the commission of any of the crimes stipulated or covered by this Law in whole or in part for the period decided by the court 3- Delete the information or data at the expense of the offender. 4- Closing the place used to perpetrate any of the crimes stipulated in this Law for a period of not less than three months and not exceeding one year. b- Whoever refrains or obstructs the implementation of any of the decisions stipulated in paragraph (a) of this Article shall be punished by imprisonment for a period of no less than three months and a fine of no less than (3000) three thousand Dinars and not more than (6000) six thousand Dinars.'

[41] Art. 44 (2) and (3) of the Jordanian Criminal Code.

such financial obligations, particularly when the offender is beyond the reach of Jordanian courts or legal processes.[42]

In summary, while Art. 31 of the Jordanian electronic crimes law aims to enhance enforcement against cybercrimes and, it has fundamental weaknesses, such as a lack of precise clarity in the concepts outlined in its provisions and insufficient procedural safeguards. There is a crucial need to ensure fairness, prevent potential misuse, and align with international human rights standards on digital rights and freedom of expression.

3. Cyber aggression crimes in the Hungarian criminal law

3.1. Introduction

Criminal offences regulated by Hungarian criminal law can be divided into three main groups, depending on whether they are characterized by being committed in cyberspace. The first group includes those traditional, long-standing crimes which can only be committed in the real world, such as homicide, assault, or rape. The second category covers the so-called 'cybercrimes in a broader sense' (or cyber-enabled crimes), which are traditional criminal offences that have migrated[43] into cyberspace but can also be committed in the real world. In this context, the information system may be the tool or place where the offence is committed or may facilitate the commission of the offence. Crimes that can also be committed in cyberspace include fraud, money laundering, drug trafficking, harassment, various verbal crimes, etc.[44] Finally, there are the so-called 'cybercrimes in a narrower sense' (or cyber-dependent crimes) which emerged with the advent of information communications technology and do not exist outside the digital world. As regards the latter category, until now there were four offences in Hungarian Criminal Code (HCC) that can be classified as cyber-dependent crimes, namely Breach of an information system or data (Art. 423), Circumvention of technical measures for the protection of the information system (Art. 424), Illegal access to data (Art. 422), and, among the crimes against property, Fraud committed by means of an information system (Art. 375). From 1 January 2025, this list was extended by one more offence, as the legislature enacted the crime titled internet aggression, which can only be committed in online space, and which is analyzed in this study.

The HCC has criminalized offences related to cyber aggression as defined in Chapter 2 of the study, even before the emergence of information communications

---

[42] Ron CHENG: Financial Sanctions and Penalties for Cybercrime. *Lawfare* June 28, 2017, https://www.lawfaremedia.org/article/financial-sanctions-and-penalties-cybercrime, 15 March 2025.

[43] Susan W. BRENNER: Re-thinking crime control strategies. *Crime Online*. (ed.: J. Yvonne). Cullompton, 2007, 12–28.

[44] Based on the above distinction, Ambrus also makes a double division in the domestic literature when he distinguishes between digital crimes in the narrower and broader sense. AMBRUS István: *Digitalizáció és büntetőjog*. Budapest, 2021, 290.

technology, in particular hate crimes, illegal acts related to disinformation or false statements and threats to commit a crime, and therefore these crimes can be considered cyber-enabled offences. Today, these offences are also increasingly committed via the internet and social media and have in common the restriction of the right to freedom of expression: when the legislature prohibits and punishes these acts, it restricts the fundamental right to freedom of expression. A further common feature is that such conduct is typically punishable when committed in public (see below).

Freedom of expression, as a fundamental right declared in the Fundamental Law of Hungary, is the mother right of several freedoms (e.g. freedom of speech, freedom of the press), it has a special role, but it is not absolute, and in certain cases it can be restricted. The Hungarian Constitutional Court applies the so-called necessity-proportionality test to assess the restriction. According to this test, 'the State may only use the tool of restricting a fundamental right if it is the only way to secure the protection or the enforcement of another fundamental right or liberty or to protect another constitutional value'. A further condition is that the restriction must meet the proportionality requirement: 'the importance of the objective to be achieved must be proportionate to the restriction of the fundamental right concerned. In enacting a limitation, the legislator is bound to employ the most moderate means suitable for reaching the specified purpose. Restricting the content of a right arbitrarily, without a forcing cause is unconstitutional, just like doing so by using a restriction of disproportionate weight compared to the purported objective.'[45] The decisions of the European Court of Human Rights (ECtHR) also have a significant impact on Hungarian criminal law and legal practice. According to the Court's practice, the shocking, outrageous or disturbing nature of an opinion alone does not justify restricting freedom of expression if no interest protected by the ECHR is harmed. However, hate speech does not enjoy the protection of Article 10, so it is necessary for democratic societies to sanction and prevent the use of expressions that incite, spread, promote or justify hatred, provided that the restriction is proportionate to the aim to be achieved. In the case of incitement to violent acts, the state also has sufficient discretion to restrict freedom of expression if it is deemed necessary in the interests of public order.[46]

Among the crimes that can be classified as cyber aggression, only incitement against a community, the crime of scaremongering, and the new offence of internet aggression mentioned above are addressed in this study. It should be noted that, in contrast to Jordanian criminal law, there is no separate Act regulating cybercrimes in Hungary, as all criminal offences, including those that can also be committed in cyberspace, are regulated by the HCC.

---

[45] Decision 30/1992 (V. 26.) AB

[46] KOLTAY András: A véleménynyilvánítás szabadsága. In: Jakab András – Fekete Balázs (szerk.): *Internetes Jogtudományi Enciklopédia.* (Alkotmányjog rovat, ed.: Bodnár Eszter – Jakab András) http://ijoten.hu/szocikk/a-velemenynyilvanitas-szabadsaga (2018). 59. 67. 69.

3.2. 'Hate speech-crime' of Hungarian criminal law: incitement against the community

3.2.1. Short legal history

Hungarian criminal law has criminalized hate speech against certain groups in society for quite a long time.[47] In 1989, at the time of the system change, the legislature created a new criminal offence titled agitation against the community. The first case of the crime was incitement to hatred against the Hungarian nation, nationality, denomination, or race (in public), and the second was the use of insulting or degrading language or other such acts. The latter case was held unconstitutional and annulled by the Constitutional Court in 1992, as it was considered to be an unnecessary and disproportionate restriction on the right to freedom of expression. Only incitement to hatred involves a danger exceeding a 'certain level' that makes it permissible to restrict the right to freedom of expression.[48] Subsequently, the legislature made several attempts to amend or redefine the statutory definition of the crime, but these were unsuccessful due to the Constitutional Court's control of the norms.[49] The Court has examined the constitutionality of the crime on several occasions, and defined how criminal liability should be balanced with the protection of the right to freedom of expression. The Court has established that criminal sanctions are only deemed to be constitutional in the case of 'acts leading to the clear and present danger of violent actions or to individual rights'. Finally, in 2016, the legislature defined incitement to violence against protected groups as a new criminal

[47] The first Hungarian Criminal Code (Act V of 1878) already punished anyone who publicly incited one class, nationality or religious denomination to hatred against another. After the Second World War, the crime of agitation, which was classified as a crime against the state, was given a strong political charge and was (also) used to punish acts against the interests of the party state.

[48] Decision 30/1992. (V. 26.) AB.

[49] An amendment to the Criminal Code from 1996 created a new criminal conduct of "other acts capable of inciting hatred" (e.g. Nazi salute). This new phrase, however, was also annulled by the Constitutional Court in 1999 on rather similar grounds as the previous decision and because the provision was indefinite [Decision 12/1999. (V. 21.) AB]. Later, a draft amendment to the Criminal Code at the end of 2003 changed the statutory definition of the crime and defined the criminal conduct as 'provoking hatred or calling for committing a forcible act'. In addition, it created a new case of the crime, when the perpetrator hurts human dignity in public by disparaging or humiliating others based on national, ethnic, racial or religious identity. The Constitutional Court declared the amendment unconstitutional in the context of a prior review of the draft act, as incitement and provocation are not synonymous. Incitement, as conduct which appeals to the emotions and instincts, is more serious than provocation, which primarily appeals to the reason and includes rational persuasion. Only incitement that incorporates a level of danger 'above a certain limit' that allows a restriction of the freedom of expression. [Decision 18/2004. (V. 25.) AB]. See in detail: András KOLTAY: *Hate Speech and the Protection of Communities in the Hungarian Legal System*. January 8, 2013, 2–3. https://ssrn.com/abstract=2197914, 15 April 2025.

conduct, in addition to incitement to hatred, and the debate on this criminal offence and its appropriate statutory definition has reached a relative calm.[50]

3.2.2. Current legislation on incitement against the community

The HCC does not use terms equivalent to the English terms 'hate crime' and/or 'hate speech'. In the Code, however, several crimes fall into this category. These include genocide, apartheid, violence against a member of the community, incitement against the community, public denial of the crimes of the national socialist or communist regimes, blasphemy against a national symbol and the use of symbols of totalitarianism.[51]

Incitement against the community is a verbal act directed against a protected group as defined by law, which in the first case is intended to create hatred in the addressees against the group or its members. In the second, more serious case, the perpetrator incites violence against the protected group.[52] As can be seen, this crime can only be committed in public, the criminal conduct is directed against protected groups or their members as defined by the Code. During the last few years, the so-called 'hate speech' against protected groups, in particular the Gypsies, Jews, LGBTQI people and migrants has been an issue of growing concern in Hungary. The question arises as to whether it is possible to express an opinion or critics on the protected groups and to what conduct against protected groups rises to the level of a criminal offence.

Based on the above, the use of abusive or degrading expression against a protected group does not constitute an incitement against the community.[53] Only the incitement to violence and incitement to hatred is considered serious enough to justify the restriction of the right to freedom of expression and the application of a criminal sanction. The interpretation of incitement to violence is relatively clear, it is nothing more than a general call for violence against a protected group. If someone writes 'Gays have no place in Hungary, let's hang them', it is the crime of incitement

---

[50] The amendment was made in October 2016 to comply with the EU Council Framework Decision on combating racism and to avoid infringement proceedings by the Commission. See: *Hungary. Responding to 'hate speech'.* 2018 Country Report, Article 19, 19.

[51] Hungary. Responding to 'hate speech', 19.

[52] Art. 332. 'Any person, who, in public, incites to violence or hatred,
a) against the Hungarian nation,
b) against a national, ethnic, racial or religious group or a member of such a group, or
c) against certain groups of the population or members or a member of such a group, in particular on grounds of disability, gender identity or sexual orientation is guilt of a felony punishable by imprisonment not exceeding three years.'
It is worth mentioning that from 1 January 2025, the new case of the crime when the perpetrator commits the mentioned incitement by, among other things, denying or challenging the commission of a war crime or crime against humanity against a protected group.

[53] For example, if someone post on the Facebook 'dirty gypsies', this may constitute defamation, but incitement against the community cannot be established.

against community. The interpretation of incitement to hatred is more difficult. These are usually false facts and information that can create anger or hatred against the protected group. If, for example, someone comments on some news about the situation of the Hungarian pensioners 'Pensioners are parasites, they don't work, they only suck our blood', this is an incitement to hatred and constitutes incitement against the community.

However, this crime is very rare in practice. Law enforcement agencies often conclude that the conduct of the perpetrator did not constitute an incitement to violence or hatred and did not create a direct threat to the protected group, so criminal proceedings are often terminated at the investigation phase, or the prosecutor does not bring charges.[54] One interesting case is worth mentioning, in which the defendant posted an advertisement on a website announcing the following as part of an event program: 'burning communist books; throwing Molotov cocktails; shooting at communists; burning red-, EU-, and LMBTQ flags.' After the court of first instance convicted, and the court of second instance acquitted him, the court of third instance found the defendant guilty of incitement against the community. According to the reasoning of the judgment, by using the term LMBTQP, he equated the LMBTQ community with pedophiles, which in itself is sufficient to incite to hatred. Furthermore, when placed in the context of throwing Molotov cocktails, the text is explicitly threatening, and burning the flag is not only capable of inciting to hatred but also violence.[55]

3.3. Crime related to disinformation in Hungarian criminal law: scaremongering

3.3.1. Background and the 'traditional case' of the crime

The crime of scaremongering was already defined in the so-called old Hungarian Criminal Code (Act IV of 1978). At this time, causing panic through disinformation was in itself a criminal offence.[56] The crime could only be committed in public, by stating untrue facts or by stating a distortion of a true fact. The latter means that the fact has an objective reality, but the communication of the fact is misleading, e.g. the perpetrator fails to disclose certain circumstances. It is important to note that it was not a criminal offence to state a true fact, even if it causes panic. Based on the old rules of scaremongering, the perpetrator committed this crime if, for example, spread the false news that 'poisoned food was found on the shelves of a shop' or 'the financial situation of the bank has weakened, and it has become insolvent.'

---

[54] Magyarországon csak ritkán fáznak rá azok, akik gyűlöletből követnek el bűncselekményt. *Index* 2017. 04. 20. https://index.hu/belfold/2017/04/20/magyarorszagon_csak_ritkan_faznak_ra_azok_akik_gyuloletbol_kovetnek_el_buncselekmenyt/?token=c978129b468d488a416cb309c2e0261b, 15 April 2025.

[55] Győr Court of Appeal, Bhar III.69/2024/9.

[56] Art. 270: 'Any person who, in public, states or reports an untrue fact or a distortion of a true fact which is suitable to cause disturbance in public peace is guilt of a felony punishable by imprisonment not exceeding one year.'

In 2000, the Constitutional Court annulled this provision of scaremongering. The Court held that the perpetrator of this conduct was acting within the scope of freedom of expression: making this conduct punishable would restrict this freedom in an unnecessary and disproportionate way and was therefore unconstitutional. However, the Court notes that it is possible to restrict freedom of expression in a state of emergency or in a state of necessity. Based on the decision of the Constitutional Court, the legislature recodified the statutory definition of the crime of scaremongering.[57] The legislator has significantly narrowed the conduct of the crime, now requiring the offence to be committed not only in public but also in a place of public danger. Moreover, the disinformation must be connected to a situation of public danger (e.g. fire, flooding). This would be the case, for example, if the perpetrator, during a flood, spreads the false news that the dams have broken, and everything will be washed away. Note that this is a theoretical example because this crime is almost non-existent in court practice.

3.3.2. The new case of the crime of scaremongering

The policy of the European Union on disinformation is based on the idea that disinformation is not illegal in itself, but it is harmful, and the European Commission has made a distinction between illegal content (such as child sexual abuse material or hate speech), and harmful content (such as disinformation).[58] However, there is a tendency in some EU Member States to make disinformation illegal and to criminalize it, and they increasingly did so during the Covid-19 pandemic.

In the spring of 2020, following the adoption of the Act on Defense against the coronavirus, the Criminal Code was also amended and a second case of the crime of scaremongering was introduced into the Code.[59] Under the new rule it is now also considered scaremongering if someone

- during a special legal order,
- in public,
- states or reports an untrue fact or distorts a true fact in any way,
- which may hinder or frustrate the effectiveness of the protective measures.

It can be seen that not only are false statements which may disturb public order now a crime, but also those which are capable of hindering or frustrating the

---

[57] Art. 337: 'Any person who, in a place of public danger, and in public, states or reports, in connection with the public danger, an untrue fact or a distortion of a true fact in a manner that is suitable to cause confusion or disturbance among a large group of people in the place of public danger is guilt of a felony punishable by imprisonment not exceeding three years.'

[58] Ronan Ó. FATHAIGH – Natali HELBERGER – Naomi APPELMAN: The perils of legally defining disinformation. *Internet Policy Review* 10 (4), 2021, 2. https://doi.org/10.14763/2021.4.1584

[59] Art. 337 (2): 'Any person who, during a special legal order and in public, states or reports an untrue fact or distorts a true fact in a manner that is suitable to hinder or frustrate the effectiveness of the protective measures is guilt of a felony punishable by imprisonment not exceeding three years.'

effectiveness of the defence (against the coronavirus in Hungary). In addition, it is no longer necessary to commit the crime at the place of a public danger, but it is enough for it to take place during a special legal order, regardless of the location. Problematic, that there is currently a state of danger in Hungary and the government is able to maintain this state for an unlimited time period.

Following the adoption of the amendment, there was a heated debate on the new case of scaremongering. Critics have most often argued that the new provision does not meet the requirement of normative clarity. Moreover, a constitutional complaint was also submitted to the Constitutional Court, asking for the annulment of the provision. According to the applicant, the provision violates

- the principle of the rule of law, in particular the requirement of normative clarity,
- the principles of necessity and proportionality, and is contrary to
- the principles of freedom of expression.

The complaint was rejected by the Constitutional Court [Decision 15/2020. (VII. 8.) AB] which held that the new provision does not violate the requirement of normative clarity, the elements of the crime can be interpreted, and this will be the duty of the courts in the application of the law. The Court also pointed out that the crime may only be committed intentionally. Consequently, the perpetrator must be aware that

- he is committing his act at the time of a special legal order;
- the fact he states is untrue or has distorted the true fact,
- his communication is capable of hindering or frustrating the effectiveness of protection.

If his intention does not extend to any of these elements, or if the statement is not objectively capable of hindering or frustrating the effectiveness of the protection, the crime is not committed according to the rules of criminal law.

3.3.3. Experience of criminal proceedings initiated for the new case of scaremongering

According to the statistics, until 14 July 2020, the police had initiated criminal proceedings for scaremongering in 134 cases. In most cases, the police decided to reject the criminal complaint or close the investigation. Only a few cases have been prosecuted and only some accused have been found guilty by the courts. In the following, we would like to mention some examples of where the offence was committed and the perpetrator was found guilty and, on the contrary, where the proceedings were terminated due to the absence of a crime.

In the first case, the perpetrator made a post with a video in the social media that 'the coronavirus does not even exist, so it is unnecessary to stay home, everyone should feel free to go out on the streets'. The perpetrator committed the crime because if people believed her, he could contribute to spread of the virus. Her communication is capable of hindering or frustrating the effectiveness of protection.[60] In the second

[60] https://hvg.hu/itthon/20210427_remhirjertesztes_koronavirus_jarvany_ozd, 15 April 2025.

case, the perpetrator worried that there is not enough protective equipment in health care facilities, so he decided to post a photo on social media with a nurse not wearing a mask. Under the picture, he wrote that "this is the situation in healthcare: there are no masks in the hospitals". The above statement could cause disturbance and hinder the defense because the perpetrator suggested that it was the general situation in the country. In the third, the perpetrator wrote in his internet-article about the mandatory wearing of masks that mouth masks are a harmful and pointless means of protection. According to the court, the perpetrator pharmacist was aware that surgical masks had already been used to prevent the spread of various infections and that masks could be used to mitigate and prevent Covid infection. In doing so, he stated untrue facts, and this conduct could hinder the effectiveness of the protection measures.[61]

In the fourth case, the accused wrote in a social media post that the government deliberately lifted the curfew at a time when the virus was at its peak. Which, in his view, could lead to mass disease. The prosecutor's office, due to the absence of crime, terminated the proceedings, saying that the post analyses a hypothetical situation and can therefore only be classified as a hypothesis and that is not capable of hindering the preventive measures.[62] In another case, the accused made the following one-sentence post on Facebook during the coronavirus epidemic: "1170 hospital beds were evacuated in the town of Gyula". He was detained for four hours; his house was searched, and his computer was seized. Later the prosecutor's office decided that the accused didn't commit a crime, the sentence was not capable of hindering the preventive measures. Moreover, his statement was later confirmed as true.[63]

In summary, it can be said that the aforementioned large number of criminal proceedings that are initiated and subsequently terminated due to scaremongering is not in itself problematic, as unfounded reports are often filed in criminal cases. The real problem arises when the investigating authority interrogates the person concerned as a suspect based on an incorrect interpretation of the statutory elements of the crime. Agreeing with the Constitutional Court, the statutory elements of scaremongering, such as what act is capable of hindering or frustrating the effectiveness of protection, are not inherently uninterpretable. The law enforcement authorities must be able to interpret these elements. It is also important that the case law on the statutory elements makes it clear from the outset that public debate and critical opinion cannot be stifled by prosecuting individuals for scaremongering. It is time for the court practice to set out specific standards for opinions published on social media.[64] It can be added that there is also an opinion in the literature that

---

61 https://magyarnemzet.hu/belfold/2022/10/dontott-a-birosag-godeny-gyorgy-remhirterjeszto, 15 April 2025.

62 https://hvg.hu/itthon/20200513_ugyeszseg_remhirterjesztes_szerencs, 15 April 2025.

63 https://media1.hu/2020/05/15/ugyeszseg-nem-terjesztett-remhirt-a-gyulai-facebookozo/, 15 April 2025.

64 András KOLTAY: On the Constitutionality of the Punishment of Scaremongering in the Hungarian Legal System. *Hungarian Yearbook of International Law and European Law* 2021 (9) 1, 42. https://doi.org/10.5553/HYIEL/266627012021009001002

scaremongering can be considered a symbolic criminal offence because it seeks to solve a social problem (the epidemic) primarily through criminal law means. Its vague elements cannot be interpreted by law enforcers, and the offence remains without practical application and will be forgotten.[65]

3.4. Internet aggression

The Hungarian legislature introduced the criminal offence of internet aggression into Hungarian criminal law on 1 January 2025.[66] The aim of the new legislation is to make online spaces safer and to reduce hate speech and incitement to violence. The values protected by the crime are public tranquility, the community's right to live free from fear and the human dignity of the people involved. The victim(s) of the offence may be an "identifiable person or persons", i.e. a particular person or group of people. It is not necessary to name the victim or victims, a reference or description is sufficient. It is also irrelevant whether the addressee is informed of the communication and expresses his or her objection to it or not.

The conduct of the crime is the use or publication of an expression (verbal communication), representation (e.g. a gif) or sound or image recording as defined by law. The use/publication may be the publication of the own expression or representation but may also be sharing (expression from another source). According to the explanatory report of the Act amending the Criminal Code, the so-called "liking" does not fall under this category, but the publication of an agreeing comment, for example, does. A further element of the criminal conduct is that the expression, the representation or the recording expresses an intention or wish to commit a future criminal act causing violent death or a particularly cruel act of violence against a specific person or persons. (In simple terms, the criminal conduct is a desire to cause the violent death or torture of another person.[67] Important to note that if the act relates to such offences committed in the past, this crime cannot be established.)

This criminal offence can be considered a cybercrime in the narrow sense, as it can be committed in public but only by means of an electronic communications network. This could be the internet, social media, but the explanatory report states that the crime

---

[65] Botos Mihály Bálint: Joggyakorlati helyzetkép a rémhírterjesztés tényállásáról. *In Medias Res* 2023/1., 183.

[66] Art. 332/A (1): Any person who, in public, uses or publishes, by means of an electronic communications network, any expression, representation, image or sound recording which expresses an intention or desire to commit a criminal act of violence
a) causing death or
b) with particular cruelty against an identifiable person or persons, if no more serious offence is committed, is guilt of a misdemeanour punishable by imprisonment not exceeding one year.

[67] In the first case, the expression must refer to a conduct that causes the deadly result unlawfully, violently and because of human intervention; the desire for events to occur independently of human intervention does not constitute the crime. In the second case, the conduct in question is a criminal offence (e.g. homicide, assault) committed with particular cruelty.

cannot be committed in a private, closed environment (for example, in a small, closed Facebook group). If the conduct does not take place by means of an electronic communications network, for example at a demonstration, a different crime may be established. Finally, the law provides for a ground for exclusion from criminal liability, namely that a person who commits the crime for the purpose of disseminating information, education, science, art or information about events in history or current affairs is not punishable, provided that the act is not suitable for creating fear.[68]

The crime is quite new in Hungarian criminal law, so there is rather limited information available on its practical application. In one case, a report was filed against an activist for internet aggression after he made the following statement about the prime minister in a video interview: 'It is not enough to remove him from office. He must be destroyed so that he cannot return.' (The proceedings are currently ongoing.)[69] In another case, after his favorite club closed down, the defendant threatened his neighbors in a comment posted on a social media site, saying he would set their houses on fire because he held them responsible for the closure.[70]

At first sight, it seems that one possible means of combating the increasingly aggressive rhetoric on the Internet and in social media could be to provide for a criminal sanction, which—imprisonment for up to one year—cannot be considered a disproportionate restriction of the right to freedom of expression. According to one criticism in the literature, the new provision provides very broad scope for application, because people often communicate impulsively and rashly on the internet. In addition, our everyday language is full of expressions which, if interpreted literally, express a desire for the death of others. On the other hand, the practical application of the crime is likely to place a significant burden on the authorities. For example, there are posts that receive hundreds of comments in a short period of time, and it is questionable whether the police are prepared to initiate proceedings in every case.[71]

3.5. Special criminal measures for combating cyber aggression crimes in Hungary: rendering electronic data permanently inaccessible and termination of a hosting service

3.5.1. Background to introducing the new criminal measures

In the case of cybercrimes, particularly some offences committed on the internet, it is essential to prevent access to illegal data and the continuation of the offence. As

---

[68] See Art. 332/A (2) of the Criminal Code.

[69] https://www.origo.hu/itthon/2025/06/feljelentettek-pankotai-lilit-miutan-orban-viktor-elpusztitasarol-beszelt, 03 July 2025.

[70] The police investigated the case for internet aggression and recommended that charges be brought, although in my opinion the act constituted the crime of harassment. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/csak-menjek-le-a-szomszedok-hazait-fel-fogom, 03 July 2025.

[71] Opinion of Szabolcs Hegyi, see: https://telex.hu/belfold/2024/12/18/online-agresszio-visszaszoritas-magyar-kormany-fidesz-torveny-komment-borton, 03 July 2025.

well as child pornography, these crimes include hate speech, misleading of consumers, copyright infringements or crimes against property committed on the internet. Until 2012, however, there was no sanction in Hungarian criminal law to make illegal content inaccessible, so the possibilities for the authorities to fight against cybercriminals were very limited.

The introduction of the new legislation was also required by Hungary's obligation based on Art. 25 of the Directive 2011/93/EU.[72] In order to comply with the obligation to harmonize criminal law, the Hungarian legislature has added a new criminal measure to the list of criminal sanctions in the new Criminal Code which consists of rendering electronic data permanently inaccessible.[73] Hungary currently has a variety of legal measures (criminal law, administrative law, civil law) for the blocking, filtering and taking down of illegal internet content.

3.5.2. Rendering electronic data permanently inaccessible: Art. 77 of the Hungarian Criminal Code[74]

In the Hungarian criminal sanction system, rendering electronic data permanently inaccessible is a security measure that may be imposed independently or together with a punishment or other criminal measure. Unlike punishments that require a culpable commission of a crime, this measure may also be applied to perpetrators who are children

---

[72] Art. 25: '1. Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavor to obtain the removal of such pages hosted outside of their territory.
2. Member States may take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.'

[73] Rendering electronic data permanently inaccessible, as a criminal sanction, may be enforced after the judgment has become final. In the case of several content-related cybercrimes, however, it is crucial to prevent the continuation of the offence by making the data inaccessible at an early stage of the criminal proceedings. This is the purpose of the new coercive measure introduced in the Criminal Procedure Code in 2013, rendering electronic data temporarily inaccessible.

[74] Art. 77 (1) of the HCC:
The data published on an electronic communications network shall be rendered permanently inaccessible, when:
a) the disclosure or publication of which constitutes a criminal offence, or
b) which is used as an instrument for the commission of the crime, or
c) which is created by the commission of a crime.
(2) The measure for permanently rendering electronic data inaccessible shall be issued even if the perpetrator cannot be prosecuted due to minority or insanity or due to other grounds for exemption from criminal responsibility, or if the perpetrator has been given a warning.

or mentally ill, and even if the perpetrator is not liable on grounds of exemption from criminal responsibility. Electronic data may be defined as data published on an electronic communications network by an electronic communications service provider that can be identified by an IP address, URL, domain name and port number.

In principle, the measure may be applied to any crime, but the Criminal Code defines the electronic data covered by the measure in a taxative manner: i) data whose disclosure or publication constitutes a criminal offence, e.g. child pornography, copyright infringements; ii) electronic data used as a tool to commit an offence. e.g. in the case of fraud committed through an information system; a fake website used by the perpetrators that resembles an Internet banking login page; iii) electronic data created by the commission of an offence, e.g., a defamatory or hate-speech communication.

Rendering the electronic data permanently inaccessible is enforceable in two ways. First, it can be done by deleting the data, which is the responsibility of the web hosting provider, who is obliged to remove the electronic data. The court specifies the hosting provider in the judgment (name, address, registered office, name of representative, etc.). The court issues a notice requiring the hosting provider to delete the data within one working day of receiving the judgment or sending the notice to the state tax authority for enforcement. If the web hosting provider fails to comply with the obligation to delete the electronic data, the court may impose a fine of between HUF 100,000 and HUF 1 million based on the notice from the tax authority. The fine may be imposed again.

Secondly, the sanction may also be carried out by permanently blocking access to the data. In this case, the court sends its judgment to the National Media and Infocommunications Authority (NMHH), which organizes and supervises the enforcement of the judgment. Electronic communications service providers who provide access to the data are obliged to block access to the electronic data. These service providers are Internet access providers (Yettel Zrt., Vodafone Zrt.), search providers (Google, Bing) and cache providers. The NMHH contributes to the prevention of cybercrimes. The Authority operates the so-called Central Electronic Database of Decisions on Rendering Data Inaccessible (KETHA). In this electronic database, the Authority stores and processes the decisions transmitted by the court and forwards them to electronic communications service providers together with search engines and caching service providers. According to the court decision, internet access providers are obliged to block access to the electronic data referred to in the decision within one working day and to filter it from Internet traffic. Search providers and cache providers are also obliged to block access to data found or stored as a result of a search for the data mentioned in the decision. If service providers fail to comply with this obligation, the court may impose the fine mentioned above.

Note that the Act on International Legal Assistance in Criminal Matters (1996) allows the Hungarian authorities, in the interest of smooth international co-operation, to use the procedural or enforcement legal assistance available to render electronic data temporarily or permanently inaccessible if the website is hosted by a foreign web hosting service provider. The Act allows the Hungarian authorities to comply

with such foreign requests for mutual legal assistance if the web hosting service provider is Hungarian.

3.5.3. Termination of a hosting service: Art. 78/A of the Hungarian Criminal Code[75]

In parallel with the introduction of a new criminal measure applicable from March 2025, a new coercive measure has also been introduced in the Criminal Procedure Code, namely the suspension of a hosting services. This means the blocking of online profiles, user accounts and websites used to commit online fraud and other cybercrimes (online aggression, online sexual offences, hate crimes, etc.) to prevent further criminal offences. The coercive measure can be ordered by the court, the prosecutor or the investigative authority during the criminal proceedings, and the person concerned cannot access the service due to its suspension and cannot conclude a new service contract, i.e. cannot create a new profile with the given service provider during the criminal proceedings. In addition, at the end of the criminal proceedings, the criminal court will permanently terminate the access of the accused to the hosting service by means of a criminal measure.

Conclusion

As the digital world becomes more central to how we live and communicate, it's no surprise that new challenges like cyber aggression have emerged. This study looked closely at how Jordan and Hungary are trying to deal with these challenges through their laws. While both countries have introduced new rules to protect people from online harm, these laws have also raised serious concerns, especially about freedom of expression on the internet.

In Jordan, the legal changes seem to give authorities a lot of power to decide what counts as harmful or offensive, which can be risky in a system where free speech is already sensitive. Hungary, while more structured in its legal language, also faces criticism that its rules could be used to silence opinions under the guise of protecting reputations.

Both frameworks reflect a delicate attempt to strike a balance between safeguarding personal dignity and ensuring the continued protection of fundamental freedoms. Nonetheless, the risk of arbitrary enforcement remains a critical issue, especially when legal texts lack precise definitions or when public authorities are given wide interpretive discretion.

This study recommends that both Jordan and Hungary revise their cyber aggression laws to provide clearer definitions and avoid vague language that could

---

[75] Art. 78/A (1) of the HCC:
'The court may order the termination of a hosting service provided to the perpetrator which he used or intended to use as an instrument for the commission of the crime.
(2) Termination of a hosting service shall be ordered even if the perpetrator cannot be prosecuted due to minority or insanity or due to other grounds for exemption from criminal responsibility, or if the perpetrator has been given a warning.'

be misused. It also urges stronger judicial oversight to ensure fair enforcement. Both countries should establish transparent appeal processes and engage in international cooperation to learn from best practices that successfully protect individuals without compromising freedom of expression. The relevant regulations in both countries adequately cover a wide range of cyber attacks, but it can be challenging for law enforcement agencies to keep track of new methods of committing crimes, and the proper categorization of individual criminal acts can cause problems in practice. It is particularly important that law enforcement agencies are aware of the latest trends in cybercrimes through up-to-date knowledge.[76]

Future research can explore practical enforcement of cyber aggression laws by examining how cases are investigated, prosecuted, and judged in both Jordan and Hungary. This would help reveal whether the laws are being applied consistently and fairly. Another important direction is public awareness and perception. Future studies could analyze how citizens understand these laws, whether they feel protected or restricted by them, and how online behavior has changed in response. This could involve surveys, interviews, or social media analysis.

References

[1] Alaeldin Mansour MAGHAIREH: Cybercrime Laws in Jordan and Freedom of Expression: A Critical Examination of the Electronic Crimes Act 2023. *International Journal of Cyber Criminology* 18/1., 2024, 15–36.

[2] AMBRUS István: *Digitalizáció és büntetőjog*. Wolters Kluver, Budapest, 2021, 1–328.

[3] Case No. 19411/2023, Judgment of 22 October 2023. *Amman Magistrate's Court Amman Magistrate Court Databases*. https://petra.gov.jo/Include/InnerPage.jsp?ID=260623&lang=ar&name=news.

[4] András KOLTAY: *Hate Speech and the Protection of Communities in the Hungarian Legal System*. January 8, 2013, 2–3. https://ssrn.com/abstract=2197914, 1–13.

[5] András KOLTAY: On the Constitutionality of the Punishment of Scaremongering in the Hungarian Legal System. *Hungarian Yearbook of International Law and European Law* 2021 (9), 1, 23–42.

[6] Ashish Kumar, SRIVASTAVA – Rakesh Kumar, SINGH: Legal Control of Right to Speech and Expression in Virtual Space. In: *Cyber Crimes in the 21st Century*. Manakin Press Pvt. Ltd., 2017. Accessed 12 March 2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4652034.

[76] DERES Petronella, A kibertérrel összefüggő bűncselekmények sajátosságai Magyarországon. *Ügyészek Lapja* 2023/1., 81.

[7] Barjes Khalil Ahmad, AL-SHAWABKEH: Criminalization of Personality Assassination via Electronic Means. *Journal of Law and Sustainable Development* 12/1., 2024, 1–20.

[8] BOTOS Mihály Bálint: Joggyakorlati helyzetkép a rémhírterjesztés tényállásáról. *In Medias Res* 2023/1., 169–185.

[9] DERES Petronella: A kibertérrel összefüggő bűncselekmények sajátosságai Magyarországon. *Ügyészek Lapja* 2023/1., 75–81.

[10] Don FALLIS, What Is Disinformation*? Library Trends* 63, 2015, 401–426. https://api.semanticscholar.org/CorpusID:13178809.

[11] E. C. TANDOC – Z. W. LIM – R. LING: Defining. Defining 'Fake News': A Typology of Scholarly Definitions. *Digital Journalism* 6, 2018, 137–153. https://doi.org/10.1080/21670811.2017.1360143

[12] *Hungary. Responding to 'hate speech'*. 2018 Country Report, Article 19, 1–62.

[13] J. M. JENKINS – K. OATLE: Psychopathology and Short-term Emotion: The Balance of Affects. *Journal of Child Psychology and Psychiatry, and Allied Disciplines* 41/4., 2000, 463–472. https://doi.org/10.1017/S0021963000005709

[14] Jillian K. PETERSON – James DENSLEY: Cyber violence: What do we know and where do we go from here? *College of Liberal Arts All Faculty Scholarship* 2017, 5/9., https://digitalcommons.hamline.edu/cla_faculty/5

[15] Jonathan CLOUGH: *Principles of cybercrime*. Cambridge, 2010, 365.

[16] Ju BINJI: Impacts of Cyberbullying and Its Solutions. *Lecture Notes in Education Psychology and Public Media* 29 (December 7, 2023), 254–258. https://doi.org/10.54254/2753-7048/29/20231521

[17] Kamil KOPECKY – René SZOTKOWSKI: Cyberbullying, Cyber Aggression and Their Impact on the Victim – The Teacher. *Telematics and Informatics* 34/2., (May 2017), 506–517. https://doi.org/10.1016/j.tele.2016.08.014

[18] KOLTAY András: A véleménynyilvánítás szabadsága. In: Jakab András – Fekete Balázs (szerk.): *Internetes Jogtudományi Enciklopédia.* (Alkotmányjog rovat, ed: Bodnár Eszter, Jakab András) http://ijoten.hu/szocikk/a-velemeny nyilvanitas-szabadsaga, 2018, 59, 67. 69.

[19] Muntaser, ALQUDAH – Ahmad, AL-AMAWI – Tawfiq, KHASHASHNEH – Hashem, BALAS: The Crime of Character Assassination in the Jordanian Cybercrime Law. *International Journal of Religion* 5/10., (July 11, 2024), 3671–3684. https://doi.org/10.61707/gsfk2s22.

[20] Naser ALRAHAMNEH: *Hate Speech in Facebook in Jordan: Survey Study*. Middle East University, Jordan, 2018. Accessed 10 March 2025. https://meu.edu.jo/libraryTheses/5ca8335e8883e_1.pdf

[21] Public Security Directorate. *The Cybercrime Unit of the Public Security Publishes Its Annual Statistics for the Year 2022*. Public Security Directorate, 2022. Accessed 5 March 2025. Available at https://bit.ly/41CKHSB.

[22] Ron CHENG: Financial Sanctions and Penalties for Cybercrime. *Lawfare* June 28, 2017. Accessed March 15, 2025, https://www.lawfaremedia.org/article/financial-sanctions-and-penalties-cybercrime.

[23] Ronan Ó. FATHAIGH – Natali HELBERGER – Naomi APPELMAN: The perils of legally defining disinformation. *Internet Policy Review* 10 (4), 2021 https://doi.org/10.14763/2021.4.1584

[24] Sakher AL-KHASAWNEH: Effect of Article 11 of the Jordanian Electronic Crimes Law on Exercising Criticism Freedom for Journalists and Workers in the Digital Media. *Journal of Law, Policy, and Globalization* 85, 2019, 48–61. https://doi.org/10.7176/JLPG

[25] Sergio Andrés SASTANO – Natalia Suarez, BETANCUR – Luz Magnolia Tilano VEGA – Harvey MAURICIO – Herrera, LOPEZ: Internet, Social Media and Online Hate Speech: Systematic Review. *Aggression and Violent Behavior* 58, 2021. https://doi.org/10.1016/j.avb.2021.101608

[26] Susan W. BRENNER: Re-thinking crime control strategies. In: *Crime Online.* (ed.: J. Yvonne) Cullompton, 2007, 12–28.

[27] *United Nations Strategy and Plan of Action on Hate Speech*. United Nations, accessed March 10, 2025. https://www.un.org/en/genocide-prevention/hate-speech/strategy-plan-action.

[28] *United Nations Strategy and Plan of Action on Hate Speech (May 2019).* United Nations Accessed 10 March 2025. https://www.un.org/en/genocide-prevention/hate-speech/strategy-plan-action.

Legislations

[1] Arab Convention on Combating Information Technology Crime (2010). Available at: [https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf] https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf 10 March 2025.

[2] Electronic Crimes Law No. 17 of 2023: *Official Gazette* 5874, 3579, dated 13-08-2023.

[3] Electronic Crimes Law No. 27 of 2015: *Official Gazette* 5343, Jordan, 5631, dated 01-06-2015.

[4] European Union, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 December 2022 on a Single Market for Digital Services (Digital Services Act), *Official Journal of the European Union* L 333, 27 December 2022, 1–75.

[5] Temporary Information Systems Crime Law No. 30 of 2010: *Official Gazette* 5056, Jordan, 5334, dated 16-09-2010.

[6] The Hungarian Penal Code (Act C of 2012 on the Criminal Code), *Hungarian Official Journal* 2012, available at: https://net.jogtar.hu/jogszabaly?docid=A1200105.TV.

[7] The Jordanian Penal Code No. 16 of 1960 and its amendments: *Official Gazette*, No. 1487, Jordan, 374. dated 1/5/1960.

[8] The Constitution of the Hashemite Kingdom of Jordan, published in *Official Gazette* Issue No. 1093, 3, January 8, 1952.