Original research article / Originalus mokslinis straipsnis
Vol. 1 No. 8 (2025): Spalis

Combating Cybercrime: Legal Aspects, Practical Challenges, and Solutions

[1] Aysel Najafli

Accepted: 09.09.2025
Published: 10.22.2025
https://doi.org/10.69760/portuni.0108007

Abstract:
The rapid development of digital technologies has not only transformed many aspects of society positively but has also generated new and complex legal challenges. Among the most serious of these is the expansion and globalization of cybercrime. As a phenomenon that transcends borders and falls outside the scope of traditional legal frameworks, cybercrime poses significant challenges to modern legal systems. This article examines the international nature of cybercrime, existing legal regulations in this field, opportunities for international cooperation, as well as the growing dynamics of cybercrime and cybersecurity issues in the era of artificial intelligence. Furthermore, it assesses the effectiveness of current normative frameworks and proposes recommendations for improving legal regulations in the future. It highlights the transnational nature of cybercrime and the need for coordinated international legal frameworks, such as the Budapest Convention. The article also discusses practical challenges in combating cybercrime (e.g., evidence collection and jurisdictional issues), reviews notable incidents (like the WannaCry and NotPetya attacks and the Cambridge Analytica scandal), and explores emerging threats including AI-enabled cyberattacks and cyberbullying. Finally, the effectiveness of existing laws and recent developments – from human rights court precedents to national strategies – are evaluated to recommend future-focused legal and policy solutions.

Keywords: *Cybercrime; Digital Threats; Transnational Crimes; Cyberbullying; Legal Regulation; Budapest Convention*

Introduction

In the digital age, the exploitation of computer networks and data for malicious purposes has created unprecedented legal challenges. **Cybercrime** generally encompasses illegal acts carried out via computer systems or the internet – from traditional offenses like fraud and theft committed online to novel crimes unique to the digital realm. These offenses are often global in reach, anonymous in nature, and technically sophisticated, complicating their detection and prosecution. Conversely, **cybersecurity** refers to the protections (technical, organizational, and legal) put in place to safeguard data and systems against such threats. Cybercrime and cybersecurity are two sides of the same coin: the former represents evolving threats, while the latter embodies the responses and preventive measures to those threats.

[1] Najafli, A. R. Lawyer, Nakhchivan, Azerbaijan. Email: ayselnecefli715@gmail.com. ORCID: https://orcid.org/0009-0008-2550-7373

Modern legal systems must adapt to the borderless character of cybercrime. Offenses committed in cyberspace frequently transcend national jurisdictions, undermining laws that are traditionally bound to territory. This has led to increased international cooperation and the creation of frameworks like the Council of Europe's *Budapest Convention on Cybercrime*, which provides a baseline for harmonizing cybercrime definitions and facilitating cross-border investigative assistance. At the same time, countries are developing national laws and strategies to protect their information space and critical infrastructure.

Addressing cybercrime is not only a technical endeavor but also a legal and societal one. Law enforcement agencies worldwide face practical difficulties in gathering electronic evidence and identifying perpetrators who exploit encryption and anonymization tools. High-profile incidents – from ransomware attacks such as WannaCry and NotPetya to large-scale data breaches like the Facebook–Cambridge Analytica scandal – have exposed gaps in readiness and regulation. Moreover, the advent of artificial intelligence (AI) is spawning new cybercrime techniques (e.g., AI-generated deepfake fraud) that existing laws struggle to cover. In the social sphere, the proliferation of cyberbullying demonstrates how digital technologies can facilitate new forms of harassment that demand legal attention.

Against this backdrop, this article examines the legal aspects of combating cybercrime, the practical challenges faced by practitioners, and potential solutions. It analyzes the efficacy of current international and national legal instruments, discusses developments in case law (including human rights implications), and explores strategies to enhance cybersecurity and resilience in the face of growing digital threats.

1. Cybercrime and Cybersecurity: Concept and Scope

The concept of cybercrime in the modern era represents a multifaceted phenomenon at the intersection of legal and technological domains. In general terms, cybercrime refers to all unlawful acts committed through computer systems, networks, and digital data. These crimes not only manifest as technological iterations of traditional offenses (e.g. fraud or theft committed via digital means) but also encompass entirely novel forms of crime unique to the digital environment and previously unknown to legal practice. Cybercrime is typically divided into several main categories:

- Crimes against computers (e.g., unauthorized system intrusion, dissemination of viruses);
- Crimes committed through computers (e.g., cyber fraud, online scams, cyberstalking);
- Illegal acquisition and dissemination of information (e.g., theft of personal data);
- Attacks targeting public and national security (e.g., cyberterrorism, assaults on critical infrastructure).

The specific characteristics of crimes committed in cyberspace – such as anonymity, global reach, and high technical complexity – significantly complicate their detection and prosecution. The role of international law in this field is becoming increasingly important; however, legal mechanisms in many jurisdictions remain incomplete or inconsistent.

Cybersecurity, on the other hand, refers to the combination of technical, organizational, and legal measures aimed at protecting data, systems, and networks in the digital environment. It extends beyond technical safeguards to include legal regulations, international conventions, and mechanisms for interstate cooperation. There is a mutual interconnection between these two concepts: cybercrime functions as a threat-generating phenomenon, while cybersecurity serves as the response mechanism to such threats. Consequently, they are often addressed in parallel within legislation and international legal instruments.

The scope of issues surrounding cybercrime and cybersecurity continues to expand, affecting all actors ranging from individual users to corporations, state authorities, and international organizations. This reality necessitates regulatory approaches not only at the national level but also at the international level.

2. International Legal Regulations: The Council of Europe Convention on Cybercrime (Budapest Convention)

Emerging technologies pose significant challenges for legal regulation. Information and communications now flow easily and rapidly worldwide, and physical borders no longer impede these interactions. Offenders increasingly operate far from the locations where their crimes have effects. However, national laws typically apply only within limited geographic boundaries. Consequently, there is a pressing need for solutions at the level of international law and the adoption of relevant international instruments.

According to the Convention's Explanatory Report, Recommendation No. (89) 9 of the Council of Europe (1989) helped harmonize national legal approaches to certain computer-related abuses (Council of Europe, 2001b). Nevertheless, to effectively combat new forms of crime in this sphere, a legally binding international instrument was required. Such an instrument needed to address not only measures for international cooperation but also substantive and procedural legal issues, as well as matters directly related to the use of information technologies (Council of Europe, 2001b).

Based on these considerations, the Budapest Convention on Cybercrime was developed with respect for human rights in the context of the emerging information society. The Budapest Convention was adopted on November 23, 2001, and remains the first – and still the most comprehensive – international legal document in this field. Its main objectives include:

- Preventing unauthorized access to computer systems;
- Ensuring the protection of data and systems;
- Strengthening interstate cooperation;
- Regulating procedures for obtaining and sharing electronic evidence.

For the purposes of the Convention, key terms are defined as follows (Council of Europe, 2001a):

a) **"computer system"** means any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of data;
b) **"computer data"** means any representation of facts, information, or concepts in a form suitable

for processing in a computer system, including a program that can cause a computer system to perform a function;
c) **"service provider"** means (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service;
d) **"traffic data"** means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

The offenses established under the Convention are categorized into four main groups:

- Offenses against the confidentiality, integrity, and availability of computer data and systems (Article 2 – illegal access; Article 3 – illegal interception; Article 4 – data interference; Article 5 – system interference; Article 6 – misuse of devices);
- Offenses related to the use of computer tools (Article 7 – computer-related forgery; Article 8 – computer-related fraud);
- Content-related offenses (Article 9 – offenses related to child pornography);
- Offenses related to intellectual property rights (offenses involving infringement of copyright and related rights).

The Convention also provides a comprehensive framework for criminal liability and sanctions, procedural law measures (such as preservation of stored data and expedited disclosure of traffic data), and mechanisms of international cooperation. It sets out principles for extradition and mutual legal assistance among parties, and it strives to synchronize member states' approaches to cybercrime and electronic evidence. These provisions collectively facilitate more effective cross-border investigation and prosecution of cybercriminals, addressing issues that were previously beyond the reach of any single nation's legal system (Council of Europe, 2001a).

3. The Transnational Nature of Cybercrime

Due to the globalization of information technology and digital networks, cybercriminals can operate from one country while targeting individuals, organizations, or even critical infrastructure in another. Such offenses frequently involve multiple states with different jurisdictions simultaneously, creating serious challenges for traditional criminal law mechanisms.

Criminal law must therefore evolve in line with technological advancements, as opportunities to abuse cyberspace have become highly complex and often well-organized, with the potential to cause significant harm to legitimate interests. Considering the inherently cross-border nature of the internet, combating such abuses requires joint and coordinated efforts at the international level (Council of Europe, 2001b).

Transnational cybercrimes are typically characterized by several features:

- The perpetrator is located in a different country than the victim or the targeted system;

- The commission of the offense involves servers and data transmission channels spanning multiple countries;
- Differing legal definitions of offenses and penalties across jurisdictions complicate the application of criminal law;
- Real-time cooperation between law enforcement agencies is often slower than the rapid pace of technological change, hindering timely evidence collection.

For these reasons, combating cybercrime is not feasible solely at the national level; it requires international legal frameworks and the joint implementation of effective mechanisms. In this context, the Budapest Convention – as the only binding international instrument specifically on cybercrime – aims to strengthen legal cooperation among member states, harmonize legal definitions, and standardize procedures for evidence gathering. Despite its importance, universal adoption of the Convention has not yet been achieved, and some major countries remain outside this framework, which continues to pose challenges for truly global enforcement.

4. Practical Difficulties in Combating Cybercrime

One of the primary difficulties in combating cybercrime lies in the collection and preservation of digital evidence. Electronic traces can be erased or manipulated quickly. For instance, in cases involving the theft of bank funds through hacking, law enforcement must gather perpetrators' IP addresses, server logs, and transaction records. Doing so requires technical expertise and strict adherence to legal procedures (to ensure evidence admissibility). Without international cooperation, investigating cross-border cybercrimes is nearly impossible, as crucial data often resides on servers in foreign jurisdictions.

The anonymity of perpetrators and their transnational operations pose additional obstacles. Cybercrimes are often carried out remotely, with hackers concealing their identities using virtual private networks (VPNs), proxy servers, the Tor network, and other anonymization tools. This not only complicates the efforts of national law enforcement agencies but also hampers international information exchange. For example, incidents of cyberbullying or personal data leaks on social networks may be orchestrated via foreign servers, making it difficult for a victim's local authorities to take direct action without assistance from abroad.

A further challenge arises from insufficient technical capacity within some law enforcement bodies. Inadequate training and a shortage of specialists in computer forensics and cybersecurity can hinder the prevention of cybercrimes and the effective analysis of digital evidence. Thus, developing professional expertise and modernizing investigative tools are of paramount importance. Police and forensic units need up-to-date technology and skills to trace sophisticated attacks, decrypt data, and attribute actions to specific actors.

Finally, the level of public awareness plays a crucial role in combating cybercrime. When citizens and organizations lack knowledge about basic cybersecurity practices – such as protecting personal data, using strong authentication, or recognizing phishing attempts – they inadvertently increase their vulnerability and complicate the work of law enforcement. For instance, inadequate user awareness

about phishing emails or fraudulent social media messages can lead to identity theft or financial fraud on a large scale. This underscores the need for widespread cybersecurity education campaigns and legal literacy initiatives. In short, improving public awareness and cyber hygiene is an essential preventive strategy complementing law enforcement efforts.

5. Real-World Examples of Cybercrime and International Responses

The dangers posed by cybercrime to society and legal systems have been vividly illustrated by several high-profile incidents. These cases have drawn international attention to both the legal and technological dimensions of combating digital crime:

- **WannaCry Attack (2017)** – The WannaCry ransomware attack in May 2017 was one of the most impactful cybercrime incidents worldwide. It was executed via a cryptoworm known as "WannaCry," which targeted computers running the Microsoft Windows operating system. WannaCry encrypted users' files and demanded ransom payments in Bitcoin to restore access. The attack crippled hundreds of thousands of computer systems across more than 150 countries. It hit the healthcare sector particularly hard; for example, hospitals within the UK's National Health Service (NHS) were forced to suspend operations (Whittaker, 2019). This incident demonstrated that cybercrime poses not only technical and economic risks but also direct threats to human welfare and safety.

- **Stuxnet Virus (2010)** – Stuxnet is a malicious computer worm discovered in 2010, believed to have been used as a cyber-weapon against Iran's nuclear facilities. It specifically targeted industrial control systems (SCADA systems), causing physical disruption to uranium enrichment processes. The sophistication of Stuxnet stunned cybersecurity experts, as it exploited multiple zero-day vulnerabilities and even sabotage of industrial equipment. This event showed that cybercrime (or cyber warfare) is no longer limited to fraud or data theft; cyberattacks can directly threaten national security and critical infrastructure. Stuxnet also sparked significant legal debate over the definitions of cyberterrorism and state-sponsored cyber warfare (CERT-IST, 2010).

- **NotPetya Attack (2016–2017)** – Petya is a family of ransomware-like malware first detected in 2016. It infects the master boot record of Windows systems, encrypts the file system table, and prevents the operating system from loading, then demands a Bitcoin ransom to undo the damage. In June 2017, a particularly destructive variant known as NotPetya was unleashed as part of a global cyberattack, primarily targeting businesses and government agencies in Ukraine. The malware spread rapidly via software update supply chains, causing widespread disruption (e.g., crippling ports and corporate networks around the world) (Greenberg, 2018). NotPetya's indiscriminate damage – estimated in the billions of dollars – highlighted the need for international norms and stronger defenses against state-linked cyber operations.

- **Cambridge Analytica Scandal (2018)** – This incident involved the unlawful collection of personal data from millions of Facebook users by the British consulting firm Cambridge Analytica for the purposes of political advertising and influence. The data was harvested

through a third-party Facebook application ("This Is Your Digital Life") developed in 2013 by a researcher, which collected not only quiz participants' data but also that of their friends. In early 2018, revelations about Cambridge Analytica's use of these data (without proper consent) for targeted political campaigns provoked a global debate on privacy and data protection. The scandal exposed legal gaps concerning the misuse of personal data, violations of privacy, and inadequate enforcement of information rights, while also highlighting the vulnerability of digital democratic processes to manipulation (Meredith, 2018). It directly influenced the strengthening of data protection laws (such as the EU's GDPR) and raised awareness of the importance of cybersecurity in protecting electoral integrity.

6. Cybercrime in the Age of Artificial Intelligence: Emerging Threats and Legal Challenges

The rise of artificial intelligence (AI) is profoundly transforming the landscape of cybercrime. Whereas many cybercrimes in the past were carried out manually by individuals or small groups, AI now enables perpetrators to conduct attacks that are faster, larger in scale, and more automated than ever.

AI provides cybercriminals with significant new capabilities across multiple dimensions:

- **Identity theft and blackmail via deepfakes:** AI-driven "deepfake" technology can generate highly realistic fake images, audio, or video of real people. Perpetrators can use deepfakes to impersonate individuals for fraudulent purposes or to create false compromising material for extortion and defamation. For example, an AI-generated video could falsely depict a person committing an embarrassing act, which criminals might use to blackmail the victim. Such cases blur the line between truth and fabrication, complicating legal standards of evidence and personal reputation rights.

- **Automated phishing and social engineering:** AI algorithms can sift through social media and other data to craft extremely convincing, personalized phishing emails or messages. These AI-generated phishing attacks can adapt language and tactics in real time to trick even tech-savvy users into divulging credentials or installing malware. The scale of phishing campaigns has increased as AI allows attackers to target thousands of individuals with tailored bait, undermining traditional user education countermeasures.

- **Adaptive malware:** AI-powered malware can learn and evolve to evade detection. Such "smart" malicious software might automatically test a target's defense systems, alter its behavior to avoid antivirus signatures, and even repair or re-encrypt itself if partially removed. This self-learning malware is harder for law enforcement and cybersecurity professionals to analyze, as it may not exhibit consistent patterns. It challenges existing legal frameworks that rely on identifying and classifying malware based on known signatures or behaviors.

- **Advanced social engineering and surveillance:** AI can analyze a person's online presence and communication style to mimic them (for impersonation) or to better predict their actions. For instance, AI tools could manage large numbers of fake social media accounts (bots) that interact with users in a seemingly authentic way, increasing the effectiveness of propaganda,

fraud, or recruitment for criminal activities. The ethical and legal implications of AI-driven social engineering are significant, raising questions about liability when algorithms, rather than humans, generate harmful content or deceits.

The use of AI in cybercrime raises several legal and ethical challenges for regulators and law enforcement:

- **Criminal liability for AI agents:** Traditional criminal law assumes a human perpetrator with intent. If an autonomous AI system commits an offense (for example, an AI bot carrying out an attack without direct real-time human commands), it becomes unclear who is legally responsible. Is it the owner of the system, the programmer who created the algorithm, or the user who deployed it? Legal systems have yet to establish clear accountability for harms caused by semi-autonomous or autonomous agents.

- **Attribution and evidence:** AI-enabled offenses may execute without leaving clear traces that point to a specific individual. An AI that continually modifies its code can make forensic analysis extremely difficult, complicating the collection of evidence that meets courtroom standards. Ensuring due process and the right to a fair trial becomes challenging when evidence is largely circumstantial or based on complex technical inference about AI behavior.

- **Regulatory gaps:** Currently, no universally accepted international legal framework specifically addresses cybercrimes committed using AI. National laws lag behind the technology; definitions of cybercrime may need expansion to cover new AI-driven modus operandi. International cooperation is also hindered by the novelty of these threats – countries are only beginning to discuss norms for the malicious use of AI in cyberspace.

In summary, the advent of AI necessitates proactive adaptation of the law. Legislators and international bodies will need to craft rules that encourage the beneficial uses of AI while penalizing and preventing its criminal abuses. This includes updating cybercrime laws to cover AI-generated content and perhaps establishing new standards for AI system accountability. As with earlier generations of cyber threats, a combination of technological, legal, and educational measures will be required to address the emerging challenges of the AI era.

7. Cyberbullying: A New Digital Form of Violence

Cyberbullying is a form of interpersonal harm that has emerged alongside the expansion of digital communication, essentially representing the online manifestation of traditional bullying behaviors. The term generally encompasses actions carried out through the internet, social media platforms, messaging apps, online games, and other digital tools with the intent to harass, humiliate, threaten, or socially exclude an individual (UNICEF, 2020).

Key characteristics of cyberbullying include:

- **Persistence:** Harmful messages, images, or posts can remain accessible online indefinitely, potentially causing long-term distress to the victim. Even after the abuse stops, previously shared content can continue to inflict harm by resurfacing or being further disseminated.

- **Anonymity:** Perpetrators often hide behind fake profiles or screen names, making it difficult for victims (and authorities) to identify and confront them. This perceived anonymity can embolden individuals to say or do things online that they would refrain from in person, often escalating the severity of abuse.

- **Borderlessness:** Cyberbullying can occur at any time of day and irrespective of location. A victim might be targeted while at home, in school, or anywhere with internet access. Because digital communications easily cross geographic boundaries, jurisdictional issues arise when, for instance, a bully in one country targets a victim in another.

In many countries, cyberbullying is not explicitly codified as a separate criminal offense. Instead, abusive online behaviors are prosecuted under existing laws such as those against harassment, defamation, intimidation, breach of privacy, or hate speech. However, there is a growing recognition that cyberbullying has unique facets that may require specific legal measures. Some jurisdictions have enacted targeted legislation:

- **Singapore:** The Protection from Harassment Act 2014 (POHA) in Singapore addresses various forms of harassment and anti-social behavior, explicitly including online harassment and stalking. Under POHA, victims of cyberbullying can seek protection orders, and perpetrators of electronic harassment or harmful communications can face criminal charges or fines (Ministry of Law Singapore, 2014).

- **New Zealand:** The Harmful Digital Communications Act 2015 (HDCA) was enacted to mitigate harm caused by digital communications. It established both civil and criminal remedies for serious online harassment, bullying, and the spread of harmful content. The Act provides measures such as court orders to take down offending material and criminalizes egregious cases (e.g., sending messages or posting material intended to cause serious emotional distress) (New Zealand Legislation, 2015).

Effectively addressing cyberbullying requires a multifaceted approach, as its impacts are psychological, social, and legal:

- **Psychological consequences:** Victims – especially children and adolescents – may suffer significant emotional and mental health effects. These include anxiety, depression, lowered self-esteem, feelings of humiliation, and even suicidal thoughts. Because the abuse can be ubiquitous and unrelenting (victims may feel there is "no escape," even at home), the resulting trauma can be severe. Long-term exposure to cyberbullying has been linked to self-harm and, tragically, youth suicides.

- **Social and educational consequences:** Cyberbullying can lead to withdrawal from social interaction and activities. Victims often experience strained relationships with friends or peers and may avoid school or work environments associated with the bullying. In academic settings, targeted students frequently show decreased concentration, declining performance, and higher absenteeism. The overall school or community climate can suffer when cyberbullying is widespread or tacitly tolerated, eroding trust and a sense of safety among members.

- **Legal consequences:** Depending on the nature of the behavior, cyberbullying incidents may violate civil or criminal laws. Online harassment might incur civil liability for defamation or invasion of privacy, especially if false statements or personal data are spread. More severe actions – such as credible threats of violence, sexual exploitation, hate-motivated abuse, or encouragement of self-harm – can trigger criminal charges under laws concerning threats, extortion, hate speech, or child protection. Notably, when bullying content is publicly posted, it complicates issues of content moderation and platform responsibility. Jurisdictions are increasingly holding social media companies accountable to remove or address harmful content quickly, and some legal systems allow victims to obtain court orders against both bullies and platform providers.

In summary, cyberbullying exemplifies how traditional social problems adapt to new technologies. While it extends familiar patterns of aggression into the online domain, its unique attributes demand enhanced awareness, updated legal tools, and active prevention efforts by schools, parents, tech companies, and lawmakers.

8. Cybercrime in the Context of European Court of Human Rights Precedents

Although the European Convention on Human Rights (ECHR) does not contain a provision explicitly addressing cybercrime, the European Court of Human Rights (ECtHR) has dealt with cases related to cybercrime issues through the lens of existing rights – primarily **Article 8** (right to respect for private and family life) and **Article 10** (freedom of expression). Key judgments illustrate how the Court balances state responsibilities and individual rights in the digital realm:

Article 8 – Right to Respect for Private Life

- *K.U. v. Finland* – This 2008 case is a landmark ECtHR precedent concerning online privacy, child protection, and the positive obligations of the state. An unknown person had posted a sexually suggestive advertisement on an internet dating site posing as a 12-year-old boy (the applicant, K.U.). Due to limitations in Finnish law at the time, the police were unable to compel the service provider to reveal the identity of the person who posted the ad, and the perpetrator remained unidentified. The Court unanimously found that Finland had violated the child's right to private life under Article 8. The judgment emphasized that children's privacy and safety online are matters of particularly acute state concern. The Court held that Article 8 can imply a **positive obligation** on states to enact laws that effectively protect individuals (especially minors) against serious invasions of privacy or other harms via the internet. In this case, Finland's failure to have a mechanism to identify the offender (due to strict data protection laws shielding the ISP from disclosure) left the child without an effective

remedy, amounting to a violation of the Convention (European Court of Human Rights, 2008). K.U. v. Finland thus underscores that maintaining anonymity on the internet should be balanced against the need to protect vulnerable users from criminal exploitation.

- *Benedik v. Slovenia* – In this 2018 case, the ECtHR examined whether a user's IP address falls under the protection of private life. Slovenian police, investigating criminal activity on the internet, obtained an individual's IP address from his internet service provider without a court order. Using the IP information, they identified and prosecuted the user (the applicant, Benedik). The Court found that even though an IP address is a sequence of numbers, it can be linked to a specific person's internet usage and thus to their private life. An IP address was deemed **personal data** protected by Article 8. The ECtHR concluded that law enforcement's access to subscriber information behind an IP address interfered with the user's private life. Moreover, the interference was not "in accordance with the law" because Slovenian law lacked clear and sufficient safeguards regulating such access. The case established that individuals have a reasonable expectation of privacy in their online anonymity, and states must provide proper legal procedures (like judicial authorization or other independent oversight) before unmasking an internet user's identity (European Court of Human Rights, 2018). Benedik v. Slovenia highlights the need for Cybercrime enforcement to respect data protection principles and due process.

Article 10 – Freedom of Expression

- *Delfi AS v. Estonia* – Decided by the Grand Chamber in 2015, this is a seminal case on intermediary liability and online speech. Delfi AS operated one of Estonia's largest news websites, which allowed readers to post anonymous comments under news articles. In 2006, an article about a ferry company drew numerous user comments, including highly offensive threats and hate speech directed at the ferry operator and others. Delfi's platform automatically published comments with minimal filtering and only removed them if notified of illegal content. The ferry operator sued Delfi, and Estonian courts found the company liable for failing to promptly remove the unlawful comments. Delfi AS appealed to the ECtHR, arguing that holding it liable violated its freedom of expression under Article 10. The ECtHR, however, upheld the national courts' decisions. It reasoned that Delfi was not a passive, neutral intermediary (like an internet platform that merely stores third-party content); rather, Delfi integrated the comments into its news service and had a degree of control (through the content management system and potential for moderation). The Grand Chamber held that imposing liability on Delfi for clearly unlawful comments (especially when the platform failed to promptly remove egregious hate speech after publication) was a justified and proportionate interference with Delfi's Article 10 rights (European Court of Human Rights, 2015). This ruling does not mean all platforms are liable for user comments, but it establishes that under certain conditions, online portals have a duty of care to address hate speech or threats in their comment sections. The Delfi case has been influential in the ongoing debate about regulating user-generated content, and it illustrates how freedom of expression online is not absolute – it does not protect speech that amounts to hate speech or incitement of violence.

In summary, ECtHR jurisprudence demonstrates that while cyber-specific provisions are absent in the ECHR, the existing human rights framework is being interpreted to address cyber issues. States have both **negative obligations** (to refrain from infringing on rights arbitrarily when fighting cybercrime) and **positive obligations** (to actively protect individuals from cyber threats). The Court's decisions urge a balance between upholding fundamental rights – like privacy and free expression – and enabling effective responses to cybercrime. Additionally, other Convention articles such as **Article 6** (right to a fair trial) and **Article 13** (right to an effective remedy) are increasingly relevant in cybercrime contexts, for instance, when considering fair trial rights in cybercrime prosecutions or ensuring victims have avenues for redress. As technology evolves, the ECtHR will likely continue to refine how traditional human rights principles apply to the digital environment.

9. National Legislation

Protecting Azerbaijan's information space from contemporary threats has become a key component of national security policy. The country's legislation establishes general legal foundations for information security and the protection of citizens' rights in the digital domain. The Constitution of the Republic of Azerbaijan provides broad protections: Article 32 of the Constitution of the Republic of Azerbaijan (1995) guarantees personal inviolability and the protection of private life, while Article 50 secures the right to freedom of information. These constitutional provisions form a basis for preventing cybercrimes and penalizing unlawful intrusions into the information environment.

In criminal law, Azerbaijan explicitly addresses cybercrime through specific provisions of its Criminal Code. Chapter 30 of the Criminal Code defines offenses such as unauthorized access to computer systems, violations of information security, and other unlawful acts involving computer data or networks as crimes. This framework is designed to protect both national security and the rights and interests of individuals and organizations. Key cybercrime offenses defined in the Criminal Code of Azerbaijan (1999) include:

- Article 271: Unauthorized access to a computer system;
- Article 272: Illegal acquisition of computer data;
- Article 273: Unauthorized interference with a computer system or data;
- Article 273-1: Creation, distribution, or use of programs or devices for committing cybercrimes;
- Article 273-2: Falsification of computer data or documents.

The social danger posed by these offenses primarily manifests as threats to information security and privacy. Unauthorized access to computer systems or data can compromise personal information and commercial secrets, undermining the confidentiality of individuals' and organizations' communications. Such acts violate constitutionally protected rights, including privacy of personal life and freedom of information. Cybercrimes can also disrupt economic activities – for example, hacking bank systems may lead to theft of funds or paralysis of financial operations, causing economic losses and eroding trust in online banking. Attacks on state information systems, likewise, represent a direct threat to national security, potentially resulting in the theft or alteration of sensitive government data.

The prevalence of cybercrimes in society can damage public confidence in the digital environment and hinder the healthy development of e-government and e-commerce initiatives.

The multifaceted social harm of cybercrimes in Azerbaijan can be summarized as follows:

- Impact on national security and leakage of state secrets or disruption of strategic infrastructure;
- Infringement of individuals' private life and personal data;
- Financial sector damage (frauds, thefts from bank accounts, system downtimes affecting businesses);
- Undermining public trust in digital services and institutions.

Accordingly, while punishing cyber offenders is essential, Azerbaijan also recognizes that protecting society from cybercrime must be balanced with safeguarding fundamental human rights, such as privacy and fair trial guarantees (Council of Europe, n.d.). Effective enforcement against cybercrime should therefore be accompanied by due process and oversight to prevent abuses.

Beyond the Criminal Code, Azerbaijan has administrative laws addressing less severe infractions in the information sphere. Chapter 32 of the Code of Administrative Offenses of the Republic of Azerbaijan provides for administrative liability in cases involving misuse of information resources or failures in information protection. For example, Article 371 of this Code covers violations of rules for using information resources (such as unauthorized use or dissemination of protected information), and Article 371-1 pertains to violations of requirements for securing critical information infrastructure, both of which carry administrative liability (Code of Administrative Offenses of the Republic of Azerbaijan, 2015). These administrative penalties serve as preventive tools and sanctions for offenses that may not rise to the criminal threshold but still pose risks to information security.

It should be noted that Azerbaijan has been proactive in developing a comprehensive cybersecurity strategy at the state policy level. By Presidential Decree No. 4060 dated August 28, 2023, the "Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027" was approved. This strategic document outlines the main objectives, principles, and priority tasks for national activities in information security and cybersecurity over a five-year period. The strategy addresses issues of both national and international significance, recognizing that the interests of individuals, society, and the state are intertwined in cyberspace. It applies to government bodies, private sector entities, non-governmental organizations, and citizens alike, calling for a coordinated approach to protecting the nation's vital information assets at all levels.

The strategy's implementation has already contributed to tangible improvements. Practical measures to build and strengthen a national cybersecurity ecosystem – such as establishing specialized response teams, improving cyber incident reporting, and investing in cybersecurity training – have improved Azerbaijan's standing in global benchmarks. For example, according to the International Telecommunication Union's Global Cybersecurity Index 2020, Azerbaijan advanced 15 places compared to previous years, achieving a score of 89.31 and ranking 40th among 194 countries (Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027,

2023). This progress reflects enhanced legal frameworks, capacity building, and international cooperation, aligning Azerbaijan with global best practices in the fight against cybercrime.

10. Conclusion

Cybercrime remains one of the most pressing challenges of the modern digital era. With the rapid advancement of information technologies and the expansion of global networks, cyber threats have grown increasingly complex, transnational, and disruptive. Consequently, combating cybercrime requires not only robust national measures but also extensive international cooperation and adaptive legal frameworks.

To effectively address cybercrime, several key considerations and recommendations emerge from the analysis above:

- **Enhancing national legislation:** Domestic laws must be continuously updated to cover emerging forms of cybercrime and to close gaps exploited by offenders. This includes criminalizing new types of harmful conduct (such as novel forms of data misuse or AI-facilitated crimes) and ensuring appropriate penalties. Laws should be technologically neutral yet flexible, enabling prosecutors and courts to address a range of cyber offenses without leaving loopholes.

- **Strengthening international cooperation:** Since cybercriminals operate across borders, no country can tackle the issue alone. It is essential to reinforce mechanisms for cross-border information sharing, mutual legal assistance, and, where applicable, extradition of cyber offenders. Wider adoption of international agreements like the Budapest Convention (and its supplemental protocols) can provide a common framework for cooperation. Additionally, real-time collaboration networks among law enforcement (such as INTERPOL's cybercrime division or Europol's EC3) should be supported and expanded.

- **Advancing technological defenses:** Legal efforts must be complemented by technical cybersecurity enhancements. States and organizations should invest in advanced defense tools – for example, AI-based intrusion detection, threat intelligence systems, and strong encryption – to protect critical infrastructure and data. Public-private partnerships can be particularly effective, as much of cyberspace is owned and operated by the private sector. Governments should work closely with tech companies and cybersecurity firms to anticipate threats and disseminate best practices widely.

- **Cybersecurity education and awareness:** A cyber-resilient society depends on informed citizens. Education systems should incorporate cybersecurity fundamentals, teaching children and young adults safe online behavior and how to respond to cyberbullying, scams, or suspicious communications. Public awareness campaigns are also crucial for the general population and businesses, focusing on common threats like phishing, ransomware, and identity theft. Increasing the overall "cyber literacy" of the population reduces the human vulnerabilities that cybercriminals frequently exploit.

- **Capacity building for law enforcement and judiciary:** Police, prosecutors, and judges should receive specialized training in cybercrime investigation and digital evidence handling. Establishing dedicated cybercrime units with sufficient expertise and resources is vital for effective enforcement. Similarly, the judiciary must be equipped to understand technical evidence and the nuances of cyber-law to adjudicate cases fairly and efficiently. International capacity-building programs (often facilitated by organizations like the Council of Europe or UNODC) can help less-resourced countries develop these capabilities and foster global consistency in cyber justice.

- **Transparency and accountability in cyberspace:** Governments and corporations alike should embrace transparency regarding cyber incidents and responses. Timely public reporting about data breaches, cyber-attacks, and enforcement actions builds trust and allows stakeholders to learn from each incident. Additionally, holding organizations accountable for negligence in cybersecurity (for instance, companies that fail to secure user data) through appropriate legal or regulatory penalties will incentivize better practices. At the same time, ensuring the accountability of state surveillance and cyber operations under the rule of law will help maintain public confidence that cybersecurity measures do not unduly infringe on civil liberties.

In conclusion, the fight against cybercrime demands a sustained and multifaceted approach. It is not merely a legal obligation of states under international or domestic law, but a collective responsibility of all stakeholders – governments, private sector, civil society, and individual users – to foster a safe digital environment. By strengthening legal frameworks, improving international collaboration, investing in security technologies, and educating users, societies can better safeguard themselves against cyber threats. These comprehensive measures will not only enhance the security of digital information and infrastructure but also uphold the rule of law and fundamental rights in cyberspace. Ultimately, effectively combating cybercrime is the only path to securing our digital future and ensuring that technological innovation can continue to advance free from the shadow of criminal misuse.

References

CERT-IST. (2010, September 8). *Stuxnet: A worm which targets SCADA systems*. Retrieved from https://www.cert-ist.com/public/en/SO_detail?code=stuxnet

Code of Administrative Offenses of the Republic of Azerbaijan. (2015, December 29). Law No. 96-VQ.

Constitution of the Republic of Azerbaijan. (1995, November 12).

Council of Europe. (2001a). *Convention on Cybercrime* (Budapest Convention). European Treaty Series No. 185.

Council of Europe. (2001b). *Explanatory Report to the Convention on Cybercrime* (Budapest Convention).

Council of Europe. (n.d.). *HELP online course on "Cybercrime and Electronic Evidence"*. Retrieved from https://help.elearning.ext.coe.int/

Criminal Code of the Republic of Azerbaijan. (1999, December 30). Law No. 787-IQ.

European Court of Human Rights. (2008). *K.U. v. Finland* (Application No. 2872/02, Judgment of 2 December 2008).

European Court of Human Rights. (2015). *Delfi AS v. Estonia* (Application No. 64569/09, Judgment of 16 June 2015).

European Court of Human Rights. (2018). *Benedik v. Slovenia* (Application No. 62357/14, Judgment of 24 April 2018).

Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Huseynov, T., Khalilov, Y., Ismayilov, N., & Aliyev, E. (2025). Classification and types of documents in the process of management activities. *Acta Globalis Humanitatis et Linguarum*, 2(3), 108–112. https://doi.org/10.69760/aghel.0250020015

Khalilov, Y. F., & Mirzazade, Y. E. (2024). The impact of detention and arrest on the presumption of innocence in the context of European Court judgments. In *Proceedings of the 8th International Scientific Conference "World Scientific Reports"* (pp. 609). Paris, France: Jean Monnet University.

Khalilov, Y. F., & Mirzazade, Y. E. (2025). Abortion: In the context of the legislation of foreign countries and the Republic of Azerbaijan. *Acta Globalis Humanitatis et Linguarum*, 2(1), 4–9.

Meredith, S. (2018, April 10). Facebook–Cambridge Analytica: A timeline of the data hijacking scandal. *CNBC*. Retrieved from https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Ministry of Law Singapore. (2014). *Protection from Harassment Act 2014* (POHA).

New Zealand Legislation. (2015). *Harmful Digital Communications Act 2015*.

Öztürk, A., & Garibli, I. (2025). The characteristics of monarchy as a form of government. *Acta Globalis Humanitatis et Linguarum*, 2(2), 117–125.

Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027 (Decree No. 4060). (2023, August 28).

UNICEF. (2020). *Cyberbullying: What is it and how to stop it*. Retrieved from https://www.unicef.org/end-violence/how-to-stop-cyberbullying

Whittaker, Z. (2019, May 12). Two years after WannaCry, a million computers remain at risk. *TechCrunch*. Retrieved from https://techcrunch.com/2019/05/12/wannacry-two-years-on/