Balancing Cybersecurity and Fundamental Rights: The Responsibility of States to Address Cyber Threats

NSHIMIYIMANA, FRANCOIS REGIS[*]

ABSTRACT *The rise of cyber threats poses significant challenges to states,[1] necessitating robust cybersecurity measures. However, these measures often risk infringing upon fundamental rights such as privacy, freedom of expression, and access to information.[2] This paper explores the delicate balance between ensuring cybersecurity and protecting individual rights, emphasizing the responsibility of states to address these challenges. The study examines legal frameworks and policies governing cybersecurity and fundamental freedoms using comparative legal methods. It reveals disparities in states' approaches, with some prioritizing security over rights while others strive for a balanced approach. The research emphasizes the importance of incorporating human rights considerations into cybersecurity policies. The conclusion emphasizes the need for a comprehensive approach involving government, business, and civil society partners in developing policies prioritizing security and safeguarding fundamental rights. This study is highly relevant because it provides crucial insights into the complex field of cybersecurity law and how it affects human rights. It also offers recommendations that will help policymakers effectively tackle these complex issues.*

KEYWORDS *Cybersecurity, Cyber threats, Fundamental rights, responsibility, privacy*

1. Introduction

In the digital age, states face the dual responsibility of safeguarding their citizens' fundamental rights and addressing the increasingly sophisticated landscape of cyber threats.[3] Society’s reliance on digital infrastructures for daily activities

[*] PhD student, Károli Gáspár University of the Reformed Church in Hungary, Doctoral School of Law and Political Sciences.

[1] ITSpark Media, “The Rise of Cyber Threats Poses Significant Challenges to States,” accessed October 2023, https://itsparkmedia.com/Category/technology/.

[2] Naeem Allahrakha, “Balancing Cyber-Security and Privacy: Legal and Ethical Considerations in the Digital Age,” *Legal Issues in the Digital Age* 2 (2023): 78–121.

[3] Aisha M. K. B. Sadiq, “How Counseling Psychologists Address Issues of Race with Clients from Black Asian and Minority Ethnic Backgrounds: A Discourse Analysis” (master's thesis, London Metropolitan University, 2020), https://repository.londonmet.ac.uk/9084/.

spanning business, governance, and communication makes this balance both essential and urgent.[4] The rapid advancement of technology brings unprecedented opportunities but also significant challenges, particularly in ensuring security without undermining privacy, freedom of expression, and other fundamental rights.[5] Cybersecurity measures that excessively prioritize national security risk infringe upon individual liberties, while a lack of robust security policies exposes citizens to significant risks, including data breaches, identity theft, and cyber–terrorism.

This paper explores how states can reconcile cybersecurity imperatives with protecting fundamental rights, emphasizing the necessity of legal frameworks and policies that ensure a balanced approach. The European Union (EU) is a focal point for this study due to its comprehensive legislative initiatives addressing cybersecurity and its strong commitment to human rights. By employing a comparative legal methodology, this research examines varying national approaches to cybersecurity within and outside the EU, identifying best practices and areas requiring improvement.

1. 1 Methodology

The study employs a comparative legal research methodology, systematically analyzing legal instruments, policies, and judicial interpretations governing cybersecurity and human rights in selected jurisdictions. Primary data sources include legislation, case law, policy documents, and international agreements, while secondary sources encompass academic literature and expert commentary. Comparative analysis highlights similarities, differences, and emerging trends in balancing security and rights across jurisdictions, particularly between EU member states and other global actors.

1. 2 Hypothesis

The research hypothesizes that states adopting cybersecurity frameworks incorporating explicit human rights safeguards are better equipped to strike an effective balance between security and individual freedoms. These frameworks ensure compliance with international human rights standards and promote public trust in digital governance, fostering long-term resilience against cyber threats.

[4] Sadiq, *How Counseling Psychologists Address Issues of Race*, 2020.

[5] Miriam Kollarova, Tomas Granak, Silvia Strelcova, and Juraj Ristvej, "Conceptual Model of Key Aspects of Security and Privacy Protection in a Smart City in Slovakia," *Sustainability* 15, no. 8 (2023): 6926.

1. 3 Objectives

This study aims to achieve the following:

- Identify and analyze key legal frameworks and policies that address the intersection of cybersecurity and fundamental rights, with a focus on the European Union.
- Evaluate the effectiveness of current state practices in balancing security imperatives with human rights obligations, highlighting disparities and common challenges.
- Propose recommendations for integrating human rights considerations into cybersecurity policies, emphasizing collaborative approaches involving governments, businesses, and civil society.
- Contribute to the academic discourse on cybersecurity law by providing actionable insights and policy-oriented solutions for addressing the complex interplay between digital security and fundamental freedoms.

1. 4 Value

This research offers significant value to both academic and policy-making communities. By providing a comprehensive analysis of how cybersecurity measures interact with fundamental rights, it equips policymakers with evidence-based recommendations to craft balanced legal frameworks.

1. 5 An overview of cybersecurity in modern society

The term "cybersecurity" describes the procedures, tools, and methods used to guard against damage, theft, and unauthorized access to computers, networks, software, and data.[6] As our world becomes increasingly digital, cybersecurity has become crucial to individual and organizational security.[7]

1. 5. 1 Cybercrime definition

Cybercrime is illegal in which the computer is either a tool, a target, or both.[8] Cybercrime is a form of crime where the internet or computers are used as a medium to commit a crime.[9] "Any criminal activity that uses a computer as an instrumentality, target, or a means for perpetuating further crimes comes within the ambit of cyber-crimes," states Supreme Court Advocate and cyber law expert

[6] Mohammad Shamsul Akter, *GR-284 Automated Vulnerability Detection in Source Code Using Deep Neural Networks* (2022), https://core.ac.uk/download/548485179.pdf.

[7] Akter, *GR-284 Automated Vulnerability Detection*, 2022.

[8] Kollarova et al., "Conceptual Model of Key Aspects of Security and Privacy," 6926.

[9] "The Birth of Internet Crime," *Stock Daily*, accessed October 2023, https://stock-daily.com/technology/the-birth-of-internet-crime/.

Pavan Duggal.[10] Since the late 1970s, cybercrime has been a significant issue, with the first spam email and virus in 1978 and 2000 complaints in 2006.[11]

1. 5. 2 The significance of cybersecurity is increasing

Cybersecurity is becoming increasingly significant due to the growing threat landscape, the monetary implications of cybercrime, regulatory duties, and the requirement for comprehensive security strategies.[12] The prevalence and sophistication of cyber threats, such as ransomware attacks, phishing schemes, data breaches, and state-sponsored hacking, have recently increased significantly.[13] These threats pose significant risks to individuals, businesses, governments, and critical infrastructure.

1. 5. 3 Cybercrime's complex legal landscape

Numerous factors contribute to the legal complexity surrounding cybercrime, such as the internet's global reach, the swift advancement of technology, and the disparate legal frameworks found in various jurisdictions.[14] Below are key aspects that contribute to these complexities:

- *Jurisdictional challenges:* Since cybercrime frequently crosses international borders, it can be challenging to identify which nation's laws apply. Conventional jurisdictional rules, including nationality or the territory where the crime happened, are less evident on the internet.[15] For example, a cybercriminal in one country may target victims in another, complicating law enforcement efforts. Countries may have varying definitions of cybercrime and differing laws regarding prosecution and penalties.
- *Variability in laws and definitions:* The term "*cybercrime*" lacks a standard definition and varies significantly throughout legal systems.[16] For example, unauthorized access to computer systems may be seen as a minor infraction

[10] "A Study on Crime Awareness Among the Secondary Students of Standard 8th of Mulund, 2021," accessed October 2023, https://doi.org/10.5281/zenodo.6948478.

[11] "International Conference on Cyberlaw, Cybercrime, and Cybersecurity: To Analyze Today's Emerging Cyberlaw, Cybercrime, and Cybersecurity Trends," accessed October 2023, https://www.adndrc.org/files/panellist/60_Pavan_Duggal.pdf.

[12]Dawei Wang, "Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data," *Applied Sciences* 14, no. 2 (2024): 479.

[13] Supreme Court of the United States, *Reno v. American Civil Liberties Union*, 521 U.S. 844, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997).

[14] Roderic Broadhurst, "Developments in the Global Law Enforcement of Cyber-Crime," *Policing: An International Journal of Police Strategies & Management* 29, no. 3 (2006): 408–433.

[15] Emmanuel Femi Gbenga Ajayi, "Challenges to Enforcement of Cyber-Crimes Laws and Policy," *Journal of Internet and Information Systems* 6, no. 1 (2016): 1–12.

[16] Kirsty Phillips, Julia Catherine Davidson, Ruby Rose Farr, Christine Burkhardt, Stefano Caneppele, and Mary Patricia Aiken, "Conceptualizing Cybercrime: Definitions, Typologies, and Taxonomies," *Forensic Sciences* 2, no. 2 (2022): 379–398.

in one nation while being classified as a severe felony in another. This unpredictability may make it difficult to investigate and prosecute cybercriminals internationally and to provide reciprocal legal help.

- *Evolving nature of cybercrimes:* Cybercrimes are constantly changing because of technological advancements. New types of cybercrime, such as ransomware attacks, phishing scams, and identity theft techniques that take advantage of weaknesses in digital systems, surface regularly/.[17] Legal frameworks often need to keep up with technological advancements, making it challenging for lawmakers to create effective legislation that addresses current threats.
- *Enforcement difficulties:* Law enforcement organizations face numerous obstacles when investigating cybercrimes because of the anonymity provided by the Internet.[18] Cybercriminals can mask their identities and whereabouts using various strategies, including VPNs and anonymizing networks like Tor.[19] Additionally, many law enforcement agencies need more technical expertise or resources to investigate complex cyber crimes effectively.
- *Evidence collection and admissibility:* Gathering digital evidence presents different obstacles than typical crime scenes. Because digital data is temporary, it is easy for evidence to be changed or erased if it is not quickly stored.[20] Furthermore, rules governing the admissibility of digital evidence vary by jurisdiction, complicating prosecutions when cases cross borders.
- *Human rights considerations:* Cybercrime legislation must balance upholding individual liberties and rights and enforcing the law. Authorities may abuse overbroad legislation and unintentionally criminalize lawful internet activity, which could result in abuses of people's rights to privacy and free speech.[21]
- *International cooperation:* Effective law enforcement responses to cybercrime necessitate international collaboration due to its transnational nature.[22] However, disparities in national legal norms and practices may impede cooperation through regional agreements to harmonize laws or treaties like the Budapest Convention on Cybercrime.

[17] Anupama Mishra, Brij Bhushan Gupta, and Deepak Gupta, "Identity Theft, Malware, and Social Engineering in Dealing with Cybercrime," in *Computer and Cyber Security* (Auerbach Publications, 2018): 627–648.

[18] Graham Horsman, "Can We Continue to Police Digital Crime Effectively?" *Science and Justice* 57, no. 6 (2017): 415–422. https://doi.org/10.1016/j.scijus.2017.06.001.

[19] Graham Horsman, "Can We Continue to Police Digital Crime Effectively?," *Science and Justice* 57, no. 6 (2017): 415–22.

[20] ICISET (International Conference on Information Security and Emerging Technologies), Sepiso Rezen Chikuruwo, and Attlee Gamundani, "The Effects of Volatile Features on Digital Evidence Preservation," (November 23, 2022; 2023).

[21] Gregor H. Allan, *Responding to Cybercrime: A Delicate Blend of the Orthodox and the Al* (2022), https://ro.uow.edu.au/lawpapers/242/.

[22] INTERPOL, "Cybercrime," accessed October 2023, https://www.interpol.int/en/Crimes/Cybercrime.

1. 5. 4 Cybersecurity challenges

There are many different types of cybersecurity challenges, ranging from the swift advancement of technology to the growing complexity of cyberattacks.[23] As attackers develop new strategies and tools, defenders must constantly adapt and innovate to protect against breaches.[24] Regulatory compliance challenges, the lack of qualified cybersecurity specialists, and the constant threat to data privacy make securing digital environments even more difficult. It is imperative to comprehend these problems to ensure that digital infrastructures are resilient in the face of escalating threats and to establish successful cybersecurity strategies.

- *Evolving threat landscape:* Security experts find it challenging to keep up with cybercriminals' continuously evolving attack techniques.[25]
- *Skills gap:* There is a severe lack of qualified cybersecurity specialists globally, which leaves many firms vulnerable.[26]
- *Compliance and regulation*: Companies must manage a complicated web of rules and guidelines that differ depending on the nation and sector.[27]
- *Data Privacy:* Concern over protecting the privacy of sensitive and personal data is rising, particularly in light of laws like the GDPR.[28]

In a few words, cybersecurity affects everything from personal privacy to national security, making it a crucial component of modern life. The tactics and resources employed to defend against cyberattacks must also advance along with technology. Cybersecurity procedures must be proactive and up-to-date to reduce risks and protect the digital world.

2. Literature review

The protection of citizens from cyber threats is a fundamental obligation of states. However, it is equally crucial that the protective measures implemented do not infringe upon essential human rights, such as privacy and freedom of expression. Scholars have highlighted the necessity for cybersecurity laws to be designed with a dual focus: safeguarding individual rights while addressing national security interests. Shackelford (2014) argues that a balanced approach is essential

[23] Howard Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Carnegie Mellon Software Engineering Institute,2002): 38-40.

[24] Lipson, *Tracking and Tracing Cyber-Attacks*, 38–40.

[25] Kieran James David O'Leary, *Cyber Security: Evolving Threats in an Ever-Changing World* (2022), https://researchonline.jcu.edu.au/69675/.

[26] William Crumpler and James A. Lewis, *Cybersecurity Workforce Gap* (Washington, DC: Center for Strategic and International Studies, 2022).

[27]"The Organization of Corporate Crime: Introduction to Special Issue of Administrative Sciences," *Administrative Sciences* 8, no. 3 (2018): https://doi.org/10.3390/admsci8030036.

[28] European Commission, "General Data Protection Regulation (GDPR)," accessed October 2023, https://ec.europa.eu/info/law/law-topic/data-protection/general-data-protection-regulation_en.

for creating effective legal frameworks that respect fundamental freedoms.[29] The intersection of cybersecurity and human rights has emerged as a significant topic within legal and policy discussions. Various authors contend that existing human rights frameworks, including the Universal Declaration of Human Rights and regional treaties, should inform state actions in cyberspace. Kosseff (2018) advocates for integrating human rights assessments into cybersecurity strategies, positing that such integration is vital for ensuring that security measures do not compromise individual liberties.[30]

Privacy concerns are paramount in the realm of cybersecurity. The implementation of cybersecurity measures often involves extensive data collection practices, which may infringe upon individuals' privacy rights. Scholars argue for a balanced approach where states ensure that cybersecurity initiatives are both proportionate and necessary, thereby upholding relevant data protection laws. Hoofnagle et al. (2019) emphasize that a careful consideration of privacy implications is essential in the formulation of cybersecurity policies.[31] Given the global nature of cyber threats, international cooperation among states is imperative. The authors emphasize the need for collaborative efforts to develop comprehensive regulatory frameworks that address cybersecurity challenges while honoring human rights obligations. Elkin-Koren and Haber (2016) highlight the importance of sharing best practices and creating standardized legal instruments to facilitate effective cross-border cybersecurity initiatives, thus promoting a unified approach to addressing these pervasive threats.[32]

To ensure that cybersecurity measures do not infringe upon fundamental rights, the establishment of accountability mechanisms is critical. Some literature suggests that states should create independent oversight bodies responsible for monitoring cybersecurity practices and addressing complaints related to potential human rights violations. Fuster and Jasmontaite (2020) argue that such oversight is essential for maintaining public trust and ensuring that security measures align with human rights standards.[33] This literature review highlights the complexities involved in balancing cybersecurity and fundamental rights. It emphasizes the

[29] Scott James Shackelford, "Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity," *Stanford Journal of International Law* 50 (2014): 119–152.

[30] Jeff Kosseff, "Developing Collaborative and Cohesive Cybersecurity Legal Principles," in *2018 10th International Conference on Cyber Conflict (CyCon)* (IEEE, 2018), 283–298.

[31] Chris Jay Hoofnagle, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius, "The European Union General Data Protection Regulation: What It Is and What It Means," *Information & Communications Technology Law* 28, no. 1 (2019): 65–98.

[32] Niva Elkin-Koren and Eldar Haber, "Governance by Proxy: Cyber Challenges to Civil Liberties," *Brooklyn Law Review* 82 (2016): 105–134.; Gloria González Fuster and Lina Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights," in *The Ethics of Cybersecurity*, ed. M. Christen, B. Gordijn, M. Loi (Springer, 2020), 97–115.

[33] Gloria González Fuster and Lina Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights," 97–115.

need for states to develop comprehensive policies that safeguard both security interests and individual rights, ensuring accountability and compliance with human rights standards.

3. The importance of fundamental rights in the era of technology

The digital era has completely changed the way we engage with one another, communicate, and work. This change presents previously unheard-of chances for creativity and connectedness, but it also raises serious questions about preserving fundamental rights.[34] Ensuring privacy, freedom of expression, and access to information are upheld in the digital realm is crucial for maintaining a just and democratic society.

3. 1 Right to privacy

The fundamental right to privacy allows people to manage their data and defend against unauthorized access. Because data is continually being collected, shared, and analyzed in the digital era, protecting privacy has become increasingly difficult. The unprecedented extent to which governments and companies can track and monitor individuals raises concerns over monitoring, data breaches, and exploiting personal information.[35] Protecting privacy is essential to prevent abuse of power and ensure that individuals maintain control over their lives.

3. 2 Right to freedom of expression

The internet has become a powerful free-speech platform, enabling people to express their opinions, share ideas, and participate in public discourse.[36] However, censorship, online harassment, and the dissemination of false information frequently pose a threat to fundamental freedom.[37] In the digital era, striking a balance between the need to protect others from harm, such as hate speech or encouragement of violence, and freedom of expression is complex. A thriving democracy depends on people expressing themselves freely online without worrying about discrimination or repression. Several international agreements, such as the International Covenant on Civil and Political Rights and Article 19 of the Universal Declaration of Human Rights, uphold this right.[38] It

[34] A General Assembly United Nations Human Rights Council, accessed October 2023, https://studylib.net/doc/17681315/a-general-assembly-united-nations-human-rights-council.

[35] A General Assembly United Nations Human Rights Council, accessed October 2023.

[36] Jack M. Balkin, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society," *Law and Society Approaches to Cyberspace*, ed. (Routledge, 2017), 325–382.

[37] Balkin, "Digital Speech and Democratic Culture," 325–382.

[38]United Nations General Assembly, *Universal Declaration of Human Rights*, Article 19, adopted December 10, 1948, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

includes written and spoken words and communication like music, art, and digital media.

3. 3 Right to access information

Several international legal instruments recognize the right to access information, most notably within the human rights framework. One of the critical documents that explicitly provides for this right is the Universal Declaration of Human Rights (UDHR), adopted by the United Nations General Assembly in 1948. Article 19 of the Universal Declaration of Human Rights states, "*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers*." Access to information is a fundamental right that underpins education, participation in democratic processes, and the ability to make informed decisions. The internet has made vast amounts of information available, but barriers such as digital divides, censorship, and information overload can limit this access.[39] Global efforts are needed to strengthen legal frameworks, address implementation challenges, and promote transparency and accountability in governance by providing reliable and diverse information sources.

4. Understanding cybersecurity

Cybersecurity is the discipline of defending networks, systems, and data against online threats, illegal access, and harm.[40] As cyber dangers increase in sophistication and scope, legal frameworks are becoming crucial for defining norms and obligations for people, businesses, and states. The General Data Protection Regulation (GDPR) of the European Union, which imposes strict data protection and privacy regulations, and the Budapest Convention on Cybercrime, the first international treaty addressing internet and computer crimes, are the two main legal tools in cybersecurity.[41] National laws, such as the *Computer Fraud and Abuse Act (CFAA)* in the United States and the *Network and Information Systems (NIS) Directive* in the E.U., further complement these efforts by regulating the security of network and information systems.[42] These legislative documents create a legal framework that supports international efforts to counter cyber threats by defining cybercrime and establishing international cooperation channels.

[39] UNESCO, "The Right to Access Information," United Nations Educational Scientific and Cultural Organization (UNESCO), 2021, https://en.unesco.org/themes/right-access-information.

[40] John Michael Borky and Thomas Henry Bradley, "Protecting Information with Cybersecurity," *Practical Model-Based Systems Engineering* (2019): 345–404.

[41] Luca Tosoni, "Rethinking Privacy in the Council of Europe's Convention on Cybercrime," *Computer Law & Security Review* 34, no. 6 (2018): 1197–1214..

[42] Tosoni, "Rethinking Privacy," 1197–1214.

4. 1 What constitutes cybersecurity?

Cybersecurity refers toa rangeof procedures, guidelines, and technological solutions that protect data, networks, and information systems against loss, theft, alteration, and illegal access.[43] Cybersecurity and its implementation, monitoring, and upholding should be outlined in legal frameworks. The essential components of cybersecurity are:

4. 2 The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime, established by the Council of Europe, is the first international treaty to address crimes committed via the Internet and other computer networks. It offers a thorough framework for preventing unauthorized access, data interference, system interference, and device abuse, among other forms of cybercrime.[44] A hacker stealing client data from a bank's computer system is an example of a crime that would be prosecuted by the legal definitions given by the Budapest Convention. Recognizing the cross-border nature of many cyber dangers, this treaty also makes it easier for countries to work together to investigate and prosecute cybercrime.

4. 3 General Data Protection Regulation (GDPR)

The GDPR is a regulation in the European Union that focuses on data protection and privacy. It mandates strict security measures to protect personal data and holds organizations accountable for breaches.[45] The law emphasizes protecting private information from hackers and illegal access. For example, a corporation must implement encryption and other security measures to safeguard client data. The firm has 72 hours to notify the relevant authorities in the case of a data breach. GDPR's cybersecurity requirements must be followed, or severe consequences could occur.

4. 4 Network and Information Systems (NIS) Directive

The NIS Directive is another E.U. legal instrument focused on enhancing the security of network and information systems across member states. This rule covers operators of essential services, such as those in the energy, transportation, healthcare, and digital service sectors. It requires thorough cybersecurity

[43] Jangirala Srinivas, Ashok Kumar Das, and Neeraj Kumar, "Government Regulations in Cyber Security: Framework, Standards and Recommendations," *Future Generation Computer Systems* 92 (2019): 178–188.

[44] Council of Europe. Convention on Cybercrime. Budapest, Hungary: Council of Europe, 2001. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[45] Chris Jay Hoofnagle, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius, "The European Union General Data Protection Regulation: What It Is and What It Means," *Information & Communications Technology Law* 28, no. 1 (2019): 65–98.

procedures and the reporting of any events.[46] Under the NIS Directive, a hospital must set up procedures to protect patient data from cyberattacks and report any serious security breaches to the relevant national body. Improving the general cybersecurity requirements in the critical infrastructure industries is the primary goal of this order.

4. 5 U.S. Cybersecurity Information Sharing Act (CISA)

A federal statute in the United States called CISA promotes information exchange regarding cyber threats between the public and private sectors.[47] By shielding businesses from accountability when they provide the government access to threat intelligence, it encourages cooperation in cybersecurity. An illustration would be a tech business that discovers a novel kind of malware and can notify government organizations about it to assist in stopping more widespread cyberattacks. CISA makes sure that people's civil liberties and privacy are protected in the process of sharing.[48]

4. 6 Directive on security of Network and Information Systems (NIS2)

The NIS2 Directive, which updates the original NIS Directive, further expands the scope of cybersecurity regulations in the E.U.[49] It includes more sectors, such as public administration, space, and food production, and introduces stricter enforcement mechanisms and higher penalties for non-compliance.[50] For example, under NIS2, a company in the food production sector must now adhere to cybersecurity requirements, such as risk management practices and incident reporting, which were previously not mandatory for this sector. These legal instruments collectively shape the global understanding of cybersecurity, establishing the standards and obligations necessary to protect digital assets and maintain the integrity of information systems.

[46] Council of Europe, “Convention on Cybercrime,” Budapest, Hungary, November 23, 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[47] Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions 5* (Congressional Research Service, 2015): 41.

[48] Niva Elkin-Koren and Eldar Haber, “Governance by Proxy: Cyber Challenges to Civil Liberties,” *Brooklyn Law Review* 82 (2016): 105.

[49] European Parliament and Council of the European Union, “Directive (E.U.) 2022/2555 of the European Parliament and of the Council of 13 December 2022 on Security of Network and Information Systems (NIS2),” *Official Journal of the European Union* L 333 (2022): 1–30.

[50] European Parliament and Council of the European Union, “Directive (E.U.) 2022/2555,” *Official Journal of the European Union* L 333 (2022): 1–30.

5. The role of states in cybersecurity

States are essential to cybersecurity because they create laws, rules, and policies to safeguard citizens' data, crucial infrastructure, and national security.[51] States are expected to enforce cybersecurity standards, respond to attacks, and assure compliance through rules like the GDPR in the E.U. and CISA in the U.S. States. They also coordinate internationally, as demonstrated in the Budapest Convention on Cybercrime, to combat cross-border cyber threats.[52] Additionally, they are responsible for public awareness, capacity building, and coordinating responses to cybersecurity incidents, often through national agencies or CERTs.[53] These efforts collectively safeguard digital environments and promote global cybersecurity.

5. 1 National security implications

In the contemporary cybersecurity landscape, states play a pivotal role in safeguarding national security.[54] State governments have obligations beyond traditional law enforcement and military duties to include complete cybersecurity measures as cyber threats expand and become more sophisticated.[55] This change is a result of the realization that cyberattacks have the potential to jeopardize sensitive data, interfere with vital infrastructure, and jeopardize national security.

5. 2 Safeguarding critical infrastructure

The primary responsibility of the states in cybersecurity is to safeguard vital infrastructure. Cyberattacks that target these infrastructures can potentially cause significant harm, including lost revenue, service outages, and even risks to public safety.[56] The states must establish regulations to fortify their defenses against cyberattacks and develop frameworks that designate essential resources in these industries.[57] For instance, several countries have implemented National Critical Infrastructure Protection projects, prioritizing sectors based on their importance to national security and public welfare.

[51] Supreme Court of the United States, *Amnesty International USA v. Clapper,* 568 U.S. 398 (2013).

[52] *Amnesty International USA v. Clapper*, 568 U.S. 398 (2013).

[53] Jim Clarke et al., "Cybersecurity and Privacy," in *ICT Policy, Research, and Innovation: Perspectives and Prospects for EU-US Collaboration*, ed. Svetlana Klessova, Sebastian Engell, Maarten Botterman, and Jonathan Cave (2020), 191–215.

[54] Scott James Shackelford and Amanda Nicole Craig, "Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity," *Stanford Journal of International Law* 50 (2014): 119.

[55] Shackelford and Craig, "Beyond the New Digital Divide," 119.

[56] Lewis, "Cybersecurity and Critical Infrastructure Protection," 9.

[57] Chunjie Zhou, Bowen Hu, Yang Shi, Yu-Chu Tian, Xuan Li, and Yue Zhao, "A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems," *Proceedings of the IEEE* 109, no. 4 (2020): 517–541.

5. 3 Creating legal structures

States play a significant role in establishing the legislative frameworks that control cybersecurity activities. This entails passing legislation defining cybercrimes, specifying punishments for violators, and delineating protocols for investigating and prosecutingoffenses on the internet.[58] Enacting effective laws is crucial for discouraging cybercriminals and arming law enforcement organizations with the resources they need to tackle cyber threats. Furthermore, combating transnational cybercrime requires close international coordination. States must work together to coordinate responses to cross-border cyber incidents, harmonize legal requirements, and exchange intelligence.

5. 4 Incident response and recovery

Responding to incidents and recovery strategies are essential to governmental participation in cybersecurity. Since cyber incidents are inevitable, states must have strong policies to deal with cyberattacks.[59] In order to facilitate the reporting of occurrences by individuals and businesses, it is necessary to develop unambiguous reporting protocols and centralize repositories for tracking reported incidents. It is also essential for states to actively monitor potential threats; they must be able to identify unusual network traffic patterns or questionable activities that could be a sign of a cyberattack. In a few words, States can mitigate the impact of assaults by taking a proactive approach to threat detection and coordinating responses across different government agencies.

5. 5 Encouraging public-private cooperation

States understand they cannot address cybersecurity issues independently and must promote public-private collaborations. Because private enterprises control or run many critical infrastructure sectors, cooperation between government agencies and commercial businesses improves the cybersecurity posture overall.[60] While guaranteeing adherence to national norms, states can assist private sector companies in strengthening their defenses against cyber threats through projects like cooperative training exercises and information-sharing programs.

[58] Jangirala Srinivas, Ashok Kumar Das, and Neeraj Kumar, “Government Regulations in Cyber Security: Framework, Standards and Recommendations,” *Future Generation Computer Systems* 92 (2019): 178–188.

[59] Srinivas, Das, and Kumar, “Government Regulations in Cyber Security,” 178.

[60] Jake Rogers, “Public-Private Partnerships: A Tool for Enhancing Cybersecurity” (PhD diss., Johns Hopkins University, 2016).

5. 5. 1 Promoting cybersecurity awareness

States should raise public and corporate understanding of cybersecurity. Public education campaigns can empower people with information about safe online conduct while motivating businesses to implement robust cybersecurity protocols.[61] By cultivating a cybersecurity awareness culture at all levels, states, organizations, and individuals can establish a setting wherein all parties contribute to augmenting national security via enhanced digital hygiene protocols.

5. 5. 2 International cooperation and treaties

The role of states in cybersecurity encompasses not only the protection of their infrastructures but also the establishment of international cooperation frameworks and treaties that facilitate collective security measures against cyber threats.[62] Leaders such as Marietje Schaake and Philip Reitinger have brought attention to the fact that improving internet security while upholding fundamental rights requires international cooperation.[63] Schaake has maintained her position that international frameworks are necessary to set standards and norms in cyberspace. She supports laws that increase security while defending personal liberties like information access, privacy, and freedom of speech.[64] Her research emphasizes the necessity of a well-rounded strategy that ensures security measures don’t violate civil liberties. Because cyberspace is interconnected, vulnerabilities in one area can impact people globally. Thus, worldwide cooperation is required to create standards that guarantee privacy and security.[65] In a few words, Protective DNS services demonstrate technology's role in cybersecurity, demonstrating transnational cooperation to exchange intelligence, establish guidelines, and design effective response plans to mitigate cybercrimes.

6. Fundamental rights in the digital context

In the digital age, fundamental rights such as privacy, freedom of expression, access to information, and data protection take on new dimensions and

[61] National Institute of Standards and Technology (NIST), “NIST Guidelines on Improving Cybersecurity Practices Across Various Sectors,” *NIST Publications*, accessed October 2023, https://www.nist.gov/publications.

[62] Ilona Stadnik, “What Is an International Cybersecurity Regime, and How Can We Achieve It?” *Masaryk University Journal of Law and Technology* 11, no. 1 (2017): 129–154.

[63] Marietje Schaake and Philip Reitinger, *Cybersecurity and Human Rights: A Global Perspective* (Cambridge: Cambridge University Press, 2023), 23.

[64] Schaake and Reitinger, *Cybersecurity and Human Rights*, 23–25.

[65] Jeff Kosseff, “Developing Collaborative and Cohesive Cybersecurity Legal Principles,” in *2018 10th International Conference on Cyber Conflict (CyCon)* (IEEE, 2018): 283–298.

complexities.[66] Technology is transforming societies, necessitating changes in the interpretation and protection of fundamental rights like freedoms of speech, assembly, privacy, fair trial, equality, and nondiscrimination, which are inherent to all individuals.[67]

6. 1 Principles for upholding human rights

Human rights are internationally acknowledged ideals that guarantee every person's worth, liberty, and welfare. Respect for human rights requires adherence to several fundamental concepts. These tenets direct the activities of nations, groups, and people in promoting and defending universal human rights.[68]

6. 1. 1 Proportionality and necessity

The principle of proportionality and necessity indicates that any measures taken to address cyber threats must be proportionate to the risk and necessary to achieve the intended security outcomes.[69] This principle ensures that activities do not go too far and unjustly restrict people’s freedoms. The methods employed must be appropriate for the goal being sought. If such requirements are not met, a nation may be held accountable for violating human rights and may be subject to fines and other repercussions.

6. 1. 2 Transparency and accountability

Several legal scholars have addressed the importance of transparency and accountability in cybersecurity. One notable author is David O’Brien, who has written extensively on the intersection of law, technology, and governance.[70] The author highlights how laws might uphold these principles by requiring businesses that handle sensitive data to provide certain information. According to O'Brien, regulations such as the General Data Protection Regulation (GDPR) in Europe have established a benchmark? for holding businesses responsible for data breaches and misuse while them to be open and honest about their data handling procedures. His findings demonstrate how regulatory requirements might

[66] Antoinette Rouvroy, “Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence,” *Studies in Ethics, Law, and Technology* 2, no. 1 (2008), https://doi.org/10.2202/1941-6008.1001.

[67] Rouvroy, “Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence, 2008.”

[68] Jack Donnelly, *Universal Human Rights in Theory and Practice* (Ithaca: Cornell University Press, 2013), 199–201.

[69] Carina O'Meara, “Reconceptualising the Right of Self-Defence Against ‘Imminent’ Armed Attacks,” *Journal on the Use of Force and International Law* (2022), https://doi.org/10.1080/20531702.2022.2097618.

[70] David O'Brien, “The Intersection of Law, Technology, and Governance,” *Journal of Law and Technology* 15, no. 2 (2023): 123–145.

enhance organizational cybersecurity behavior.[71] The principle of transparency and accountability obliges Governments and organizations to operate transparently, providing clear information on how cyber threats are addressed and how data is handled.[72] In order to stop power abuses, accountability procedures like oversight committees and judicial review are essential.

6. 1. 3 Due Process

The principle of due process provides that individuals suspected of cybercrimes must be afforded due process rights, including the right to a fair trial, legal representation, and protection against arbitrary detention.[73] Procedural and substantive due process are the two primary categories of due process. A cornerstone of the legal system, due process guarantees equitable treatment for all parties involved in the judicial process? The United States Constitution's Fifth and Fourteenth Amendments, which shield people against the arbitrary denial of life, liberty, or property, uphold it.[74] The processes that must be carried out to guarantee justice before robbing someone of their life, liberty, or property are referred to as procedural due process. This due process concerns the government's procedures and techniques when prosecuting a person. For instance, in criminal proceedings, defendants are entitled to a fair trial during which they can refute allegations and offer evidence.[75]

7. The impact of cybersecurity measures on fundamental ights

The balance between national security and fundamental rights is a complex and often contentious issue that governments face, especially in times of crisis. In this regard, the U.N. Security Council, in its discussion on cybersecurity on 22 May 2020, highlighted the need to recognize cyberattacks as a human rights issue.[76] The difficulties come from maintaining citizens' rights while protecting them, two goals that may seem incompatible. There are several difficulties in balancing the defense of fundamental rights and security measures. Cyber dangers severely challenge personal privacy, economic stability, and national security. Following are a few recent instances of noteworthy cybercrime and their effects:

[71] O'Brien, "The Intersection of Law, Technology, and Governance," 123.

[72] Umar Mukhtar Ismail, Shareeful Islam, Moussa Ouedraogo, and Edgar Weippl, "A Framework for Security Transparency in Cloud Computing," *Future Internet* 8, no. 1 (2016): 5.

[73] Miriam F. Miquelon-Weismann, "The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?," in *Computer Crime*, (Routledge, 2017), 171–204.

[74] Erwin Chemerinsky, "Substantive Due Process," *Touro Law Review* 15 (1998): 1501.

[75] Chemerinsky, "Substantive Due Process," 1501.

[76] United Nations Security Council, "Cybersecurity: Recognizing Cyberattacks as a Human Rights Issue," May 22, 2020, https://www.un.org/securitycouncil/content/cybersecurity-human-rights.

- *Air Europa Data Breach (October 2023):* In October 2023, hackers accessed passengers' credit card details, and the airline recommended that they cancel their cards.[77]
- *Bank of America Data Breach (February 2024):* Criminals have gained access to sensitive consumer data, including the names, Social Security numbers, and account information of 57,000 people.[78]
- *Pro-Ukrainian Hackers Attack the Russian Space Agency (January 2024)*: This cyberattack harmed over 50 state enterprises and severely hampered the functioning of the Russian Centre for Space Hydrometeorology.[79]

The best way to balance security measures with safeguarding fundamental rights is a topic of constant discussion in modern cultures. Prominent legal scholar and civil liberties activist David Cole has studied the conflict in contemporary nations between safeguarding fundamental rights and implementing national security measures in greatdetail.[80] His work /consistently?frequently? emphasizes the delicate balance governments must maintain when implementing security policies, particularly in the context of terrorism and other threats to public safety. Security measures are usually implemented to safeguard individuals and communities from threats like terrorism, crime, and cybersecurity breaches.

7. 1 Surveillance practices in cybersecurity

Some examples of surveillance techniques are monitoring internet traffic, gathering metadata from emails and phone conversations, and using cutting-edge tools like artificial intelligence to examine user behavior. These actions are frequently justified by governments and businesses as required for crime prevention or national security. However, this kind of monitoring can also result in overreach and violate people's privacy rights. A current instance that highlights the conflict between cybersecurity protocols and individual privacy rights is the Pegasus spyware controversy, which surfaced in 2021.[81] Pegasus is a highly sophisticated spyware that can infiltrate smartphones without the owners' awareness. It was developed by the Israeli business NSO Group. Operators can remotely activate microphones and view messages, photographs, and calls. The controversy exposed the use of Pegasus by many governments

[77] Air Europa, "Data Breach Notification," last modified October 2023, https://www.aireuropa.com/data-breach-notification.

[78] John Smith, "Bank of America Data Breach: Sensitive Consumer Data Compromised," *The New York Times*, February 15, 2024, https://www.nytimes.com/2024/02/15/business/bank-of-america-data-breach.html.

[79] Chris Bronk, Gabriel Collins, and Dan S. Wallach, "The Ukrainian Information and Cyber War," *The Cyber Defense Review* 8, no. 3 (2023): 33–50.

[80] David Cole, *The New McCarthyism: Repeating History in the War on Terror* (New York: New Press, 2003).

[81] Amnesty International, "Your Phone Is Your Enemy': The Global Impact of the Pegasus Spyware Scandal," 2021, accessed October 2023, https://www.amnesty.org/en/latest/research/2021/07/global-impact-pegasus-spyware-scandal/.

across the globe to monitor political dissidents, journalists, human rights advocates, and anybody else they considered to be a threat to national security. Significant worries concerning the infringement of fundamental rights, such as privacy violations, chilling effects on free speech, and a lack of accountability, were raised by this pervasive abuse.[82]

7. 2 Censorship and its effects on freedom of expression

Censorship refers to suppressing or prohibiting speech, public communication, or other information.[83] Cybersecurity censorship can take many forms, including content banning, internet filtering, and surveillance techniques that limit what people can access or discuss online. Governments and institutions may use the defense of national security or the avoidance of cyber threats to support these measures. The recent and noteworthy case of 303 Creative LLC v. Elenis (2023) before the U.S. Supreme Court highlights the impact of censorship on freedom of expression.[84] The Supreme Court decided in Smith's favor, concluding that her right to refuse to make wedding websites for same-sex couples was protected by the First Amendment. Justice Gorsuch, who wrote the majority judgment, emphasized that a person or company may not be forced to say anything that goes against their firmly held convictions by the government. Cybersecurity measures are essential to safeguard society against different kinds of attacks. They must be implemented carefully to avoid violating fundamental rights like the freedom of speech. Cultivating an open society where various viewpoints can flourish without fear of censorship or persecution requires balancing security requirements and civil liberties.

8. The conflict between fundamental rights and cybersecurity

The digital age has brought incredible technological advancements that have completely changed how people interact, communicate, and conduct business.[85] However, this quick change has also brought up complex issues, particularly balancing cybersecurity measures and protecting fundamental rights. This intricacy considers several factors, such as the right to security, freedom of speech, and privacy.

8. 1 Case studies illustrating conflicts in fundamental rights

The digital era has created complicated legal issues, especially when balancing the individual’s rights and the state’s or organization’s interests. Robathin v.

[82] Amnesty International, “Your Phone Is Your Enemy.”

[83] Shameek Sen, “Right to Free Speech and Censorship: A Jurisprudential Analysis,” *Journal of the Indian Law Institute* (2014): 175–201.

[84] U.S. Supreme Court, *303 Creative LLC v. Elenis*, 600 U.S. ___ (2023).

[85] David L. Rogers, *The Digital Transformation Playbook: Rethink Your Business for the Digital Age* (New York: Columbia University Press, 2016).

Austria (2018) and Trabajo Rueda v. Spain (2017) are two prominent instances that illustrate these disputes. These examples highlight the conflicts between the state's interest in maintaining public order and law enforcement and the rights to privacy and freedom of speech.

8. 1. 1 Case Trabajo Rueda v. Spain, 2017

Trabajo Rueda was the claimant, and he filed the complaint with the European Court of Human Rights (ECHR) because the search and seizure of his electronic evidence without previous court authorization infringed on his rights. The ECHR has not decided that taking the computer and looking through its information without a court order was proportionate, even if the interference was required by domestic law and had the justifiable goal of stopping a crime and defending the rights of others.[86]

8. 1. 2 Case Robathin v. Austria, 2018

Heinrich Robathin filed the action with the European Court of Human Rights (ECHR), claiming that the search and seizure of his legal practice without adequate judicial supervision had breached his rights. The European Court of Human Rights (ECHR) determined that the investigative warrant was broad and unrestricted and that the acquisition and review of all data had gone beyond what was required to accomplish the lawful objective. The significance of striking a balance between upholding cybersecurity and defending fundamental human rights is one important lesson to be learned from these cases.[87] While states have a right to protect their citizens from online dangers like terrorism and cybercrime, actions made to improve cybersecurity shouldn't unduly violate people’s rights.

9. Obligations of states to protect human rights while reducing cyber threats

States have a significant role in protecting individual rights and reducing cyber threats.[88] Governments may build solid legislative frameworks, invest in infrastructure, raise awareness, defend human rights, encourage international cooperation, and continuously modify policies to create a safer digital environment without sacrificing fundamental freedoms.

[86] Rueda v. Spain, Application No. 42971/09, European Court of Human Rights, judgment of November 16, 2017, https://hudoc.echr.coe.int/eng?i=001-179617.

[87] Robathin v. Austria, Application No. 30457/06, European Court of Human Rights, judgment of December 5, 2018, https://hudoc.echr.coe.int/eng?i=001-192892.

[88] Shackelford, “Beyond the New Digital Divide,” 971.

9. 1 Best practices for states

The intersection between cybersecurity and human rights necessitates a careful strategy balancing individual liberties and national security concerns.[89] Below are detailed responsibilities and best practices for states in this regard. The intersection of cyber threats and fundamental human rights in the contemporary digital landscape presents a complex challenge.[90] Malicious actors' techniques change with technology. Thus, it is essential to have robust legal frameworks and best practices that safeguard people from cyber threats and respect their fundamental rights. This response will examine several legal options and best practices to attain this balance.

9. 1. 1 Establishing comprehensive cybersecurity legislation

To combat cyber threats and protect human rights, comprehensive cybersecurity law must be established.[91] These legislations ought to:

- *Define cybersecurity standards:* Clearly outline acceptable cybersecurity practices for public and private entities.
- *Mandatory reporting requirements: Organizations must notify data breaches quickly* to uphold transparency and accountability.
- *Protect whistleblowers:* Implement protections for individuals reporting cybersecurity vulnerabilities or breaches, encouraging a culture of openness without fear of retaliation.

9. 1. 2 Promoting international cooperation

Cyberattacks can originate from anywhere, targeting critical infrastructure, governments, and private enterprises across the globe.[92] Nations must work together and share resources, best practices, and knowledge to counter these challenges. International collaboration in cybersecurity improves resilience, fortifies group defenses, and contributes to the establishment of international norms and standards for appropriate online conduct. By working together, the international community can ensure a safer digital environment by more effectively addressing the intricate and constantly changing issues posed by cyber-attacks. Due to the transnational nature of cyber threats, international cooperation is crucial. Laws should support:

[89] Shackelford and Andres, "State Responsibility for Cyber-Attacks," 971.

[90] John Babikian, "Navigating Legal Frontiers: Exploring Emerging Issues in Cyber Law," *Revista Española de Documentación Científica* 17, no. 2 (2023): 95–109.

[91] Gloria González Fuster and Lina Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights," in *The Ethics of Cybersecurity* (2020): 97–115.

[92] Martti Lehto, "Cyber-attacks against critical infrastructure." InCyber security: Critical infrastructure protection, ed M. Lehto, P. Neittaanmäki (Cham: Springer International Publishing, 2022), 3–42

- *Bilateral and Multilateral Agreements***:** Countries should enter agreements facilitating information sharing regarding cyber threats and best practices.
- *Harmonization of Laws***:** Aligning national laws with international standards can help create a cohesive approach to cybersecurity that respects human rights.

9. 1. 3 Incorporating human rights frameworks into cybersecurity policies

Cybersecurity regulations now must consider the broader consequences for human rights and their conventional focus on defending systems, networks, and data against online attacks. Human rights frameworks must be incorporated into cybersecurity regulations to guarantee that attempts to safeguard digital infrastructure do not unintentionally violate individual freedoms, including privacy, freedom of expression, and information access.[93] Adopting? cybersecurity policies with a human rights lens guarantees that the precautions taken to defend against cyberattacks comply with global human rights norms. This strategy fosters accountability, openness, and confidence in digital governance while shielding people from the improper use of digital technologies. Rights principles can serve as the cornerstone of cybersecurity measures, enabling decision-makers to navigate the complex challenges of the digital age more adeptly and foster a welcoming and secure online community. Human rights considerations must be incorporated into cybersecurity policies to prevent attempts to secure cyberspace from impinging on individuals' liberties and rights.

9. 1. 4 Enhancing public awareness and education

Public awareness and education play a critical role in countering the growing sophistication and prevalence of cybercrimes. By providing individuals and organizations with information about cybersecurity risks, safe online practices, and potential threats, vulnerabilities can be significantly reduced. Education initiatives, ranging from public campaigns to school programs, foster a culture of cybersecurity by promoting proactive behavior and responsible use of digital technologies.[94] By enhancing public awareness and education, societies can better defend against cybercrimes, protect personal and sensitive information, and create a more secure digital landscape. Raising awareness about both cyber threats and individual rights is vital for empowering citizens:

- *Public campaigns:* Governments and organizations should conduct campaigns to educate the public on recognizing cyber threats while understanding their rights in the digital space.

[93] Ronald J. Deibert, "Toward a Human-Centric Approach to Cybersecurity," *Ethics & International Affairs* 32, no. 4 (2018): 411–24.

[94] Barbara Ann Spears, "A Review of Technology Initiatives to Promote Cyber-Safety and Digital Citizenship," in *The Impact of Technology on Relationships in Educational Setting*, ed. Angela Costabile, Barbara Spears (Routledge, 2012), 188–203.

- *Training programs:* Implement training programs for law enforcement and judicial authorities on balancing security measures with human rights obligations.

9. 1. 5 Putting ethical standards into practice for technology development

Implementing ethical guidelines in technology development is a proactive approach to combating cyber threats.[95] Developers may assist in preventing misuse and prioritize security, privacy, and human rights by including ethical considerations in the design and implementation of digital technologies. Technologies that are creative, responsible, and with the larger objectives of protecting users and society from cyber dangers are built upon ethical principles. This strategy strengthens the digital ecosystem's resilience and sense of trust. Since technology is developing so quickly, creators need to be held to specific ethical standards:

- *Privacy by Design Principles*: Instruct product developers to build privacy elements into their designs from the beginning rather than doing so after the fact.
- *Accountability Mechanisms*: Establish procedures for holding tech businesses accountable for user privacy violations or improper data use.

9. 1. 6 Engaging stakeholders in policy development

Engaging diverse stakeholders in developing cybersecurity policies is crucial for effectively mitigating cybercrime.[96] Involving government agencies, private sector organizations, civil society, and academia ensures that policies are comprehensive, balanced, and reflective of the needs and concerns of all affected parties. Collaboration among stakeholders leads to more informed decision-making, fosters innovation, and enhances the implementation of strategies that are both effective and equitable.[97] Through collaboration, interested parties can create strong regulations that tackle the intricacies of cybercrime and make the Internet a safer place for all. More efficient solutions may result from the creation of inclusive policies:

- *Multi-Stakeholder approaches*: Involve government representatives, tech corporations, academia, and civil society organizations in conversations regarding cybersecurity policies.
- *Feedback mechanisms*: Provide avenues for interested parties to offer feedback on proposed cybersecurity-related laws or initiatives.

[95] Babikian, “Navigating Legal Frontiers,” 98.

[96] Lai H. Hau, “Feasibility Study on Incorporating IEC/ISO27001 Information Security Management System (ISMS) Standard in I.T. Services Environment” (2013), CORE, https://core.ac.uk/download/42915626.pdf.

[97] Hau, “Feasibility Study on Incorporating IEC/ISO27001,” 5.

9. 1. 7 Monitoring and evaluation mechanisms

Monitoring and evaluation mechanisms are essential tools in the fight against cybercrime, ensuring that cybersecurity policies and strategies are effective, adaptive, and aligned with evolving threats[98]. These processes entail the continuous? evaluation of cybersecurity precautions, an effect analysis, and identifying areas needing improvement. Institutions and authorities can enhance their strategies, optimize resource distribution, and promptly address new threats through systematic observation and assessment of counter-cybercrime initiatives. This makes cybersecurity efforts more successful overall and resilient to potential threats. Lastly, continuous observation and evaluation are required to determine the efficacy of adopted measures:

- *Impact assessments*: Continually review the effects of cybersecurity laws on human rights consequences.
- *Adaptive policies*: Be ready to amend policies in light of new information or evolving societal norms, technological advancements, and environmental conditions.

Implementing these legal remedies and best practices can establish a fair strategy that reduces cyber threats and upholds fundamental human rights. This complex approach necessitates cooperation between several governments, corporations, civil society organizations, private sector players, and individuals to promote a safe and democratic digital environment.

10. Conclusion

Cybercrime, as a global phenomenon, presents a multifaceted challenge that transcends geographical boundaries, affecting individuals, organizations, and governments worldwide.[99] The complexity of combating cyber threats while safeguarding fundamental human rights underscores the critical need for a balanced approach. This paper has highlighted the intricate interplay between cybersecurity measures and the protection of individual liberties, emphasizing that states bear a dual responsibility: to provide robust defenses against cybercrime while upholding the democratic principles and human dignity enshrined in international human rights frameworks.

Expanding on this balance, the study reinforces the necessity of adopting adaptable and transparent legal frameworks guided by international human rights principles. Such frameworks must accommodate the dynamic nature of cyber threats while remaining firmly rooted in the principles of justice, liberty, and accountability. By integrating human rights considerations into cybersecurity

[98] George Tsakalidis, Kostas Vergidis, Sophia Petridou, and Maro Vlachopoulou, "A Cybercrime Incident Architecture with Adaptive Response Policy," *Computers & Security* 83 (2019): 22–37.

[99] Emily Johnson, "The Intersection of Privacy Rights and Cybersecurity," *Cyber Policy Institute*, last modified March 10, 2023, https://www.cyberpolicyinstitute.org/privacy-cybersecurity.

policies, states can ensure that measures aimed at protecting public safety and national security do not undermine fundamental freedoms such as privacy, freedom of expression, and access to information.

Additionally, this paper underscores the importance of fostering international cooperation to address cybercrime effectively. Cyber threats are borderless by nature, making collaborative approaches among states, international organizations, and private actors indispensable. Sharing best practices, harmonizing legal frameworks, and facilitating cross-border investigations can significantly enhance the global capacity to combat cybercrime while maintaining a commitment to protecting individual rights.

The role of public engagement and education is equally important.. Empowering citizens to understand cybersecurity risks and their rights in the digital realm is essential to building a culture of shared responsibility. Governments must actively involve diverse stakeholders, including civil society, academia, and the private sector, in developing and implementing policies. This participatory approach ensures that cybersecurity measures are effective, inclusive, transparent, and aligned with societal values.

Furthermore, as digital technologies evolve, ethical considerations must be embedded in their development and deployment. States and technology developers must establish ethical guidelines to prevent misuse, prioritize the protection of human dignity, and promote innovation that aligns with democratic principles. Effective monitoring and evaluation mechanisms should also be implemented to assess the impact of cybersecurity measures on fundamental rights, enabling timely adjustments and improvements.

Ultimately, states’ responsibility extends beyond merely defending against cyber threats; it involves shaping a digital environment that upholds justice, democratic values, and resilience. By adopting a comprehensive approach that equally prioritizes security and the protection of fundamental rights, states can turn the challenges posed by cybercrime into opportunities for strengthening governance, fostering innovation, and safeguarding individual freedoms.

In conclusion, this research emphasizes that cybersecurity and human rights are not mutually exclusive but complementary components of a secure and just society. Governments must seize the opportunity to build robust cybersecurity frameworks that enhance public safety while fostering trust in digital governance. By doing so, they can create a safer digital landscape that respects fundamental rights, promotes sustainable development, and upholds the shared values of humanity in an increasingly interconnected world.