Cybersecurity Protection Committee
(CPC)

ASMUN VIII

Presidents

Angelo Colonna
Maria Jose Penagos

Barranquilla, Colombia

Table of Content:

I. Welcoming Letter

Dear Delegates,

It is an honor to welcome you all to ASMUN VIII. We are Angelo Colonna, and Maria Jose Penagos and it is a privilege for us to serve as Chairs in the Cybersecurity Protection

Committee, where we will embark on a journey of diplomacy, debate, and impactful decision-making. As we gather here, we are not just participants in a Model of United Nations; we are thinkers, problem-solvers, and advocates for change.

Through the committee, we will delve into complex global issues that demand not only knowledge but also creativity, collaboration, and a deep sense of responsibility. Every decision made, every resolution drafted, and every argument presented contributes to a greater understanding of the world we aim to shape.

We encourage each delegate to engage with passion, integrity, and respect for different perspectives. Diplomacy is not about winning an argument; it is about finding solutions that are sustainable, balanced, and just. This model is an opportunity to challenge your viewpoints, and most importantly, take ownership of your voice and your future. Whether this is your first debate session or one of many, make the most of every moment.

If you need any guidance, do not hesitate to contact us. We are here to ensure that this is not just an academic exercise, but a grateful experience.

Best of luck, and let's make this experience a remarkable one.

"A person who never made a mistake never tried anything new."

- Albert Einstein

Angelo.colonna@americanschool.edu.co

Whatsapp: 3173192290

II. Introduction to the Committee

2.1 History

The Cybersecurity Protection Committee (CPC) was established as a proactive initiative to address the constantly evolving landscape of cybersecurity threats and data protection challenges in today's digital age. As technology progresses at an unprecedented pace, the risks associated with cybercrime, data breaches, and unauthorized access to sensitive information also escalate. The CPC serves as a forum for informed discussions, strategic policymaking, and global collaboration aimed at mitigating these risks and fostering a secure online environment.

The formation of the CPC was driven by the escalating demand for an international framework to combat the increasing sophistication of cyber threats. Over the past decade, cyberattacks have become more frequent and severe, targeting government institutions, financial systems, healthcare sectors, and private corporations. The emergence of ransomware, phishing schemes, AI-enabled cyber warfare, and data privacy violations has underscored the urgent need to create a dedicated platform to address these critical concerns.

Although cybersecurity has long been a priority for individual nations and private entities, the absence of standardized global regulations and collaborative strategies has often left vital systems exposed. Acknowledging this shortcoming, the CPC was created to foster international cooperation among key stakeholders, promoting best practices, ethical guidelines, and proactive measures to cultivate a safer and more resilient digital landscape.

A hallmark of the CPC is its focus on proactive cybersecurity measures rather than merely reactive solutions. The committee advocates for preventive strategies such as establishing robust encryption standards, developing AI-driven threat detection systems, launching cybersecurity awareness campaigns, and formulating regulatory policies that can adapt to the ever-changing cyber threat landscape. Furthermore, the CPC emphasizes individual digital responsibility and promotes education on secure online practices for both organizations and citizens alike.

2.2 Organization and Functions

The Cybersecurity Protection Committee (CPC) is structured to provide an inclusive, interdisciplinary, and action-oriented approach to tackling the challenges of cybersecurity and data protection in the digital age. Unlike traditional committees that focus primarily on state actors and diplomatic negotiations, the CPC engages a wide range of stakeholders, including CEO's, government representatives, cybersecurity specialists, and representatives from international organizations. This diversity ensures a holistic and practical approach to addressing cybersecurity concerns that impact both the private and public sectors.

In the CPC, delegates assume the role of decision-makers and thought leaders, advocating for the interests and cybersecurity policies of their respective organizations or countries. Whether representing a country, a multinational corporation, or a cybersecurity firm, delegates are expected to contribute to discussions with expert knowledge, real-world case studies, and forward-thinking solutions. Their role extends beyond simply defending their organization's stance; they must also engage in deep analysis of cyber threats, emerging trends, and ethical dilemmas that affect the global digital landscape.

The CPC is divided into specialized working groups, each focused on a specific domain of cybersecurity. These groups may include:

1. Data Privacy and Protection: Examines regulations, best practices, and technological advancements for safeguarding personal and corporate data.

2. Cyber Threat Intelligence and Response: Analyzes global cyber threats, including malware, ransomware, phishing, and nation-state cyberattacks.

3. Ethical and Legal Frameworks: Discusses the legal implications of cybersecurity policies, international cyber laws, and ethical concerns surrounding digital surveillance and AI in security.

Throughout the committee sessions, delegates must defend their positions, negotiate agreements, and propose innovative solutions that align with the principles of global cooperation, digital sovereignty, and technological resilience.

One of the core responsibilities of the CPC is to bridge the gap between technical expertise and policy implementation. Cybersecurity is not merely a technical issue but also a legal, economic, and ethical one. Delegates are encouraged to explore solutions that balance security, privacy, innovation, and human rights, ensuring that proposed cybersecurity strategies are both effective and justifiable in a global context.

2.3 Mission and Vision

The mission of the Cybersecurity Protection Committee (CPC) is to promote global cooperation in safeguarding digital environments by addressing emerging cybersecurity threats and ensuring the protection of personal data. We aim to foster responsible digital practices among nations and technology leaders, advocate for transparent data management, and develop comprehensive strategies to protect users from the evolving risks of cyber warfare and online vulnerabilities.

Our vision is to create a safer and more transparent digital world where privacy is respected, cybersecurity threats are minimized, and all nations and organizations collaborate to ensure the responsible and ethical use of technology. We strive to build a future where individuals and institutions can interact freely and securely in the digital space, protected from exploitation and cyber threats.

III. Topic A: The Illusion of Digital Privacy: The Behind-the-Scenes Management of Our Data.

3.1 Introduction

In the digital age, the concept of privacy has become increasingly complex and fragile. While users navigate the internet under the impression that their personal data is protected, much of their information is being collected, analyzed, and monetized without their explicit awareness. This phenomenon, often referred to as "The Illusion of Digital Privacy," highlights the gap between perceived and actual privacy in the online world.

Behind every click, search, and social media interaction, a vast ecosystem of data management operates invisibly. Technology giants, digital service providers, and third-party entities collect user data for various purposes—ranging from targeted advertising and algorithm optimization to governmental surveillance. Although privacy policies and data

protection regulations exist, many users remain unaware of the extent to which their data is harvested and how it is utilized.

This issue is not only a matter of individual privacy but also raises critical questions about ethics, transparency, and accountability. With the rapid evolution of artificial intelligence and big data analytics, the ability to monitor and manipulate digital behaviors has expanded, posing significant risks to civil liberties. Countries with strong data protection frameworks, like the European Union's General Data Protection Regulation (GDPR), contrast sharply with regions where digital privacy remains largely unregulated, further exacerbating global disparities.

As the lines between public and private digital spaces blur, the need for international cooperation and robust regulatory frameworks becomes more urgent. This topic aims to explore the mechanisms behind the collection and management of personal data, evaluate the effectiveness of existing regulations, and propose solutions to bridge the gap between digital innovation and the protection of individual privacy.

3.2 Historical Background

The debate over digital privacy began in the late 20th century with the rise of personal computing and the advent of the internet. In the 1990s, as online communication and e-commerce grew, concerns about how personal information was collected and used became more pronounced. This era saw the introduction of early data protection laws, such as the United States' Privacy Act of 1974 and the European Union's Data Protection Directive of 1995, which laid the foundation for regulating data collection and ensuring user privacy.

The early 2000s marked a turning point with the emergence of social media platforms like Facebook, Twitter, and Google. These companies adopted business models heavily reliant on user data to drive targeted advertising and personalize user experiences. This period also saw the rapid expansion of data collection practices, often without users' full understanding or consent. High-profile data breaches and revelations about government surveillance, such as those exposed by Edward Snowden in 2013, highlighted the extent of mass data collection and raised global awareness of digital privacy issues.

In response to these growing concerns, governments and international bodies began to implement stronger data protection regulations. The European Union's General Data Protection Regulation (GDPR), enacted in 2018, became a landmark legal framework mandating transparency, user consent, and accountability for data handling. Similar laws followed worldwide, including the California Consumer Privacy Act (CCPA) in the United States and the Personal Data Protection Act (PDPA) in Singapore.

Despite these regulatory advancements, challenges persist. The rapid evolution of artificial intelligence, data analytics, and emerging technologies continues to outpace legal frameworks. Additionally, many regions lack comprehensive data protection laws, leaving millions vulnerable to exploitation. The ongoing tension between technological innovation and privacy protection remains a critical issue, making international dialogue and cooperation essential to address the complexities of digital privacy in the 21st century.

Today, digital privacy remains a pressing concern as technology continues to evolve and data collection practices become increasingly sophisticated. Despite the implementation of regulatory frameworks, major data breaches, unethical data practices, and a lack of transparency continue to pose significant risks to individuals' privacy.

One of the most prominent cases in recent years is the Cambridge Analytica scandal (2018), where the personal data of approximately 87 million Facebook users was harvested without their consent. This data was used to influence political campaigns, including the 2016 U.S. presidential election and the Brexit referendum. The scandal exposed major gaps in user privacy protection and sparked global calls for stronger regulations.

Another critical issue is the rise of surveillance capitalism, a term describing how companies like Google and Meta profit from collecting and analyzing user data to sell targeted advertisements. Despite the existence of privacy policies, many users are unaware of the scale at which their online behavior is tracked. In 2023, Meta faced a $1.3 billion fine from the European Union for violating GDPR rules by transferring European users' data to the United States without adequate protection.

Additionally, government surveillance programs remain a significant threat to digital privacy. The U.S. National Security Agency (NSA) and similar agencies in other countries continue to collect vast amounts of personal data under the guise of national security. In countries like China and Russia, extensive state-led surveillance programs monitor online communications and restrict digital freedoms.

Emerging technologies such as artificial intelligence (AI) and biometric data collection raise further privacy concerns. AI-driven systems can analyze personal information on an unprecedented scale, while facial recognition technologies used by both private companies and governments heighten fears of mass surveillance. In 2021, Amazon's Ring was criticized for sharing private security footage with law enforcement without user consent, raising questions about corporate responsibility and individual privacy.

While some countries enforce strict data protection laws, others lack comprehensive regulations, creating global disparities in privacy standards. For example, while the European

Union enforces GDPR, regions such as Africa and Southeast Asia remain vulnerable due to weak or nonexistent privacy legislation. This fragmented legal landscape allows corporations to exploit regulatory loopholes and limits the enforcement of privacy rights on a global scale.

The ongoing challenge lies in balancing technological innovation with the protection of individual privacy. As digital ecosystems grow more complex, international cooperation, corporate accountability, and stronger regulatory frameworks are essential to bridge the gap between digital advancement and the safeguarding of personal data.

3.4 Guiding Questions

1. How can governments and international organizations effectively enforce data protection regulations across borders?

2. What measures can be implemented to increase transparency in data collection practices by tech companies?

3. How can countries with weak or nonexistent data protection laws be supported in developing stronger regulatory frameworks?

4. To what extent should technology companies be held accountable for data breaches and unethical data use?

5. How can the balance between national security and individual privacy be maintained in the face of increasing surveillance?

6. What role should artificial intelligence regulation play in protecting user privacy?

7. How can public awareness be increased to empower users to protect their digital privacy?

8. Should there be a global standard for digital privacy protection, and if so, how could it be implemented?

9. What are the potential risks of emerging technologies like biometric data collection and how can they be mitigated?

10. How can the international community address the disparity between countries with strong privacy protections and those without?

3.5 Glossary of Terms

Algorithm Bias	Algorithm bias refers to systematic errors in automated systems that result in unfair outcomes, often disadvantageous to certain

	groups based on factors like race, gender, or socioeconomic status..
Artificial Intelligence (AI)	AI is a branch of computer science that focuses on creating intelligent machines capable of learning from data, reasoning, and making decisions.
Biometric Data	Biometric data refers to unique physical or behavioral characteristics, such as fingerprints or facial recognition, used for authentication and identification.
Consent Management	Consent management involves obtaining and managing user consent for the collection and processing of their personal data, in compliance with privacy regulations.
Data Breach	A data breach is an unauthorized access, disclosure, or acquisition of sensitive data, often resulting in the exposure of personal information.

Data Privacy	Data privacy refers to the protection of personal information from unauthorized access or disclosure. It encompasses practices, regulations, and technologies aimed at safeguarding sensitive data.
Deep Learning	Deep learning is a subfield of machine learning that uses neural networks with multiple layers to process and analyze complex data, such as images and text.
Encryption	Encryption is the process of converting data into a secure, coded format that can only be accessed or read by someone with the correct decryption key. It is used to protect sensitive information, ensuring privacy and security during storage or transmission.
GDPR (General Data Protection Regulation)	GDPR is a data privacy law enacted by the European Union (EU) that governs how organizations collect, store, and process personal data. It aims to protect individuals' privacy and gives them greater control over

	their personal information, with strict guidelines and penalties for non-compliance.
IoT (Internet of Things)	IoT refers to a network of physical devices, such as appliances, sensors, and other objects, that are connected to the internet. These devices collect, share, and exchange data, allowing for remote monitoring, automation, and improved efficiency across various industries.
Machine Learning	Machine learning is a subset of AI that involves the development of algorithms that enable computers to learn and make predictions or decisions without explicit programming.
Privacy by Design	Privacy by design is an approach to system development that prioritizes data privacy and protection from the outset, rather than as an afterthought.

VII. Topic B: The Rise of AI-Powered Cyber Warfare: Are We Prepared for the Invisible Enemy?

4.1 Introduction

In today's rapidly evolving technological landscape, the rise of artificial intelligence (AI) has revolutionized many sectors, including cybersecurity and warfare. AI's integration into cyber warfare introduces new challenges and threats, creating what many experts now describe as an "invisible enemy." Cyberattacks driven by AI are not only faster and more autonomous but also increasingly sophisticated. These attacks can exploit vulnerabilities in critical infrastructure, disrupt national security, and even manipulate entire societies. As AI continues to develop, the question remains: Are we truly prepared for the invisible enemy and face the risks it posses?

4.2 Historical Background

Cyber warfare, though a relatively modern phenomenon, has evolved over the past few decades as technology has advanced. Early examples of cyberattacks included incidents like the 2007 cyberattack on Estonia, which demonstrated the potential for state-sponsored cyber warfare to target a nation's infrastructure and disrupt daily life. These early attacks were primarily carried out by human hackers, using traditional methods of malware and phishing schemes.

However, with the rise of AI, the landscape of cyber warfare has changed. AI technology enables far more sophisticated and automated attacks that can learn and adapt on their own, making detection and prevention significantly more difficult. Early examples of AI-driven cyber threats have already been seen, including self-replicating malware, AI-powered ransomware, and autonomous bots used in cyber espionage. Over time, the growing dependence on digital systems and AI technologies has raised concerns over the vulnerability of critical infrastructure and military systems to such AI-driven cyber attacks.

Incidents(?):

In 2007, Estonia experienced a series of cyberattacks following a diplomatic dispute with Russia. Government, financial, and media websites were targeted, rendering online banking and communication systems inoperative. The attacks were traced to Russian IP addresses, prompting NATO to establish the Cooperative Cyber Defence Centre of Excellence in Tallinn in response.

(Foto)

In 2008, Georgia faced cyberattacks coinciding with military conflicts over South Ossetia. Websites of Georgian government agencies and media outlets were disrupted, illustrating the integration of cyber operations with conventional warfare.

(Foto)

The sophistication of cyberattacks escalated with the emergence of AI technologies. In 2017, the WannaCry ransomware attack affected approximately 200,000 computers across 150 countries, exploiting vulnerabilities in Microsoft Windows. Later that year, the NotPetya attack, originating in Ukraine, caused over $10 billion in damages worldwide.

(Foto)

In 2024, reports indicated that hackers from China and Iran were leveraging AI tools, such as Google's Gemini, to enhance their cyberattacks. These AI-driven methods included writing malicious code, identifying vulnerabilities, and conducting targeted research, marking a significant shift towards more intelligent and adaptive cyber threats.

(Foto)

The increasing use of AI in cybercrime was further highlighted by a 2024 United Nations report, which revealed that Southeast Asian cyber scammers utilized AI and advanced technologies to steal up to $37 billion in 2023. These scams encompassed fraudulent investment schemes, cryptocurrency fraud, and the use of deepfakes, demonstrating the diverse applications of AI in malicious activities.

In response to these evolving threats, nations are bolstering their cybersecurity measures. In 2024, Britain announced the establishment of a laboratory dedicated to countering Russian cyber threats, particularly those involving AI. The initiative aims to develop advanced defenses against AI-enhanced cyberattacks, reflecting the growing recognition of AI's role in modern warfare.

4.3 Current Situation

As of now, AI-powered cyberattacks are no longer just hypothetical threats but a real and growing concern. Countries like the United States, China, and Russia are known to have invested heavily in developing AI-based cyber capabilities. These nations are not only building AI for defensive cybersecurity but also for offensive operations. The ability of AI to autonomously analyze vast amounts of data, identify vulnerabilities, and carry out cyberattacks in real-time has created a new dimension in warfare.

Currently, AI is being used in several ways within the cyber domain:

Autonomous malware: Programs that can evolve and adapt to bypass security measures.

Deepfake technology: AI-generated fake videos and audio to manipulate information and sow confusion.

AI-based ransomware: Ransomware that can automatically target specific high-value systems or organizations, maximizing the damage it causes.

The future of autonomous weapons systems has already seen shocking outcomes. For example, in March 2020 an autonomous drone in Libya, the Turkish-made Kargu-2 quadcopter, killed a human being—without any input from a human operator. The incident occurred during a conflict between Libyan government forces and a breakaway military faction led by the Libyan National Army. It reignited ongoing concerns in the U.S. and other countries about how much human oversight AI-powered weapons should have. The killing was a potential first in warfare, in which an attack drone designed to provide tactical

intelligence, surveillance, and reconnaissance capabilities for ground troops struck with no apparent human control.

International norms and regulations surrounding AI-driven cyber warfare are still in their infancy. Many nations are playing catch-up, trying to bolster their defenses, but the rapid pace of technological advancement is outpacing legislative and policy frameworks. This has led to a dangerous gap in cybersecurity and international diplomacy, as the global community has yet to develop a clear and unified strategy to combat AI-driven cyber threats.

4.4 Guiding Questions

1. What are the main risks associated with AI-powered cyber warfare, and how might they affect my country/delegation ?

2. How can my country/delegation ensure the ethical use of artificial intelligence in cybersecurity without violating privacy rights?

3. Should there be international regulations governing the use of AI in cyber warfare, similar to the Geneva Conventions?

4. How can can my country/delegation strengthen their cybersecurity defenses to prepare for AI-driven cyberattacks?

5. What role should international organizations, like the United Nations, play in promoting cybersecurity cooperation between nations?

6. Can AI be used to defend against cyberattacks as effectively as it can be used to launch them?

7. What are the potential consequences of a large-scale AI cyberattack on critical infrastructure like power grids or hospitals?

8. How should my country/delegation balance national security concerns with the need for global cooperation in the digital age?

9. What measures can be taken to protect civilians from the impacts of AI-driven cyber warfare, which might include disruptions to daily life or access to essential services?

10. Should there be a global treaty to prevent AI cyberattacks, and what consequences should there be for those who violate it?

4.5 Glossary of Terms

Autonomous malware	Malicious software that can autonomously replicate, evolve, and adapt to avoid detection and exploit vulnerabilities in computer systems.
Cyber espionage	The use of cyber tools to steal sensitive or classified information from government or corporate entities, often for political or economic gain.
Cyber warfare	The use of digital attacks to disrupt, damage, or destroy a country's or organization's critical infrastructure, often

	with the intent of causing harm or gaining an advantage.
Deepfake	AI-generated media (video, audio, or images) that manipulate real content to mislead or deceive audiences by creating realistic but fabricated scenarios.
Ransomware	A type of malicious software designed to block access to a computer system or data until a ransom is paid.

V. Expectations and Recommendations from the Chair

The committee expects delegates to be prepared and thoroughly informed on the topics to be discussed, taking into account information from both historical and current events, and to connect with the different aspects, points of view, and factors that will influence the flow of the debate within the committee.

Given that the committee's objective is to discuss strategies to strengthen cybersecurity and formulate security policies adapted to the cyber threat, delegates are expected to provide strong and effective leadership to provide strategic guidance to achieve this objective.

Delegates are expected to be able to express their opinions diplomatically, respectfully, and convincingly, and to deliver insightful interventions even though the topics to be discussed are based on conspiracy theories. Well-crafted presentations supported by reliable sources are expected, not only to discuss the benefits but also the consequences that these could bring to humanity. Taking this into account can significantly contribute to shaping the different strategies during the debate.

We also recommend doing in-depth research and watching interviews, conferences, or speeches if possible to effectively interpret your assigned role. We have high expectations for you and look forward to a fluid, oratory-filled, and engaging debate. We wish you the best of luck!

VI. Delegations and Positions

1. Mark Zuckerberg – CEO of META

Position:

META advocates that data collection is essential for personalizing user experiences and delivering targeted advertising. Although the company has introduced privacy controls like the "Off-Facebook Activity" tool, it faces ongoing criticism for its extensive data collection practices and privacy breaches. Mark Zuckerberg supports self-regulation and opposes overly restrictive laws that could hinder innovation.

Stance on Regulation:

Supports minimal regulation to maintain innovation but opposes strict frameworks like the GDPR, claiming they limit technological progress.

2. **Elon Musk – Owner of X (Formerly Twitter)**

Position:

Since acquiring X, Musk has promoted free speech and reduced content moderation, raising concerns about privacy and data protection. He believes that strict data privacy regulations stifle innovation and limit open discourse.

Stance on Regulation:

Opposes heavy regulation on digital privacy, favoring a more open and less restricted approach to data usage and freedom of expression.

3. **Sundar Pichai – CEO of Google**

Position:

Google argues that data collection is vital for improving its services and advancing artificial intelligence. Despite introducing privacy initiatives like Privacy Sandbox, the company faces fines for unauthorized data transfers. Pichai supports a balanced approach that fosters innovation while respecting user privacy.

Stance on Regulation:

Advocates for unified global privacy standards instead of fragmented national regulations but resists rules that limit service personalization.

4. **Tim Cook – CEO of Apple**

Position:

Apple champions user privacy as a fundamental right. The company has implemented features like App Tracking Transparency, restricting third-party data collection. Tim Cook actively supports stronger privacy laws to protect consumers.

Stance on Regulation:

Supports comprehensive data protection regulations and argues that companies should be held accountable for safeguarding user information.

5. **Satya Nadella – CEO of Microsoft**

Position:

Microsoft emphasizes ethical data usage and transparency. The company has implemented strong internal privacy frameworks and supports responsible AI. Nadella believes that data privacy is a core responsibility for tech companies.

Stance on Regulation:

Favors clear, enforceable global privacy regulations that balance innovation and consumer protection.

6. **Sam Altman – CEO of OpenAI**

Position:

OpenAI prioritizes ethical AI development and transparency. Altman has warned about the risks of unregulated AI and supports initiatives that protect user data while fostering technological innovation.

Stance on Regulation:

Advocates for international collaboration on AI and data privacy policies, ensuring both innovation and user protection.

7. **Shou Zi Chew – CEO of Tik Tok**

Position:

TikTok faces scrutiny over its ties to China and potential data sharing with the Chinese

government. Shou Zi Chew emphasizes the platform's commitment to data localization and transparency measures.

Stance on Regulation:

Supports data transparency but opposes policies that could jeopardize user engagement or platform growth.

8. **Neal Mohan – CEO of YouTube**

Position:

YouTube relies heavily on data-driven advertising. Mohan has advocated for better user privacy controls while maintaining the company's ad-supported business model.

Stance on Regulation:

Supports user privacy initiatives but is cautious of regulations that could disrupt online content and advertising ecosystems.

9. **Jeff Bezos – Founder of Amazon**

Position:

Amazon's business model relies on extensive customer data for personalized marketing. Bezos has expressed concerns about excessive regulation but acknowledges the importance of protecting consumer trust.

Stance on Regulation:

Opposes overregulation but supports voluntary industry standards and self-regulation for data handling.

10. **Jensen Huang – CEO of NVIDIA**

Position:

NVIDIA's primary focus is on AI and data analytics. Huang emphasizes the responsible use of AI and the importance of protecting user data, particularly in emerging fields like machine learning.

Stance on Regulation:

Advocates for balanced regulations that enable AI innovation while protecting personal data.

11. Evan Spiegel – CEO of Snapchat

Position:

Snapchat emphasizes privacy through ephemeral messaging and data minimization. Spiegel has supported greater transparency while defending the need for creative freedom on digital platforms.

Stance on Regulation:

Supports privacy protections but opposes rigid policies that could limit innovation and user engagement.

12. United States

Position:

The U.S. balances national security interests with corporate innovation. While there are sector-specific regulations (e.g., California Consumer Privacy Act – CCPA), there is no unified federal data privacy law. Agencies like the NSA conduct mass surveillance under programs like PRISM, raising global concerns.

Stance on Regulation:

Opposes global regulations that limit national security programs but supports corporate accountability and voluntary data transparency frameworks.

13. China

Position:

China has one of the world's most comprehensive surveillance systems. The Cybersecurity Law (2017) and Personal Information Protection Law (2021) allow the government to access and monitor user data for national security.

Stance on Regulation:

Supports state-controlled data governance and opposes international regulations that undermine domestic authority over digital privacy.

14. United Kingdom

Position:

The UK enforces robust data protection through the UK GDPR but allows surveillance under the Investigatory Powers Act (IPA), which grants broad intelligence-gathering powers.

Stance on Regulation:

Advocates for strong data protection standards while defending the state's right to conduct surveillance for national security.

15. Russia

Position:

Russia enforces strict data localization laws through the Federal Law on Personal Data,

requiring companies to store citizens' data within national borders. It uses extensive digital surveillance for political control.

Stance on Regulation:

Opposes international regulation of domestic surveillance and promotes sovereign control over national digital infrastructure.

16. India

Position:

India's **Digital Personal Data Protection Act (2023)** emphasizes data localization and user privacy but allows government surveillance for public safety.

Stance on Regulation:

Supports national data sovereignty while advocating for balanced regulations that ensure both privacy and technological growth.

17. Brazil

Position:

Brazil enforces the **General Data Protection Law (LGPD)** to protect personal data and ensure transparency. It supports international cooperation on digital privacy.

Stance on Regulation:

Advocates for global privacy standards while maintaining the ability to regulate tech companies operating within its borders.

18. Germany

Position:

Germany enforces the **GDPR** and advocates for strict privacy protections. The country opposes mass surveillance and promotes consumer rights over corporate interests.

Stance on Regulation:

Strongly supports international privacy regulations and holds tech companies accountable for user data protection.

19. Colombia

Position:

Colombia's Statutory Law 1581 (2012) regulates personal data protection. However, weak enforcement mechanisms make the country vulnerable to privacy violations and cyber threats.

Stance on Regulation:

Supports stronger international cooperation to protect user data and improve local cybersecurity frameworks.

20. Japan

Position:

Japan enforces the Act on the Protection of Personal Information (APPI) and collaborates with international bodies to maintain data security while fostering technological innovation.

Stance on Regulation:

Supports global privacy standards but advocates for policies that do not restrict technological advancements and data-sharing agreements.

21. South Korea

Position:

South Korea has one of the world's most comprehensive data privacy frameworks under the Personal Information Protection Act (PIPA). It prioritizes user privacy while allowing limited government surveillance.

Stance on Regulation:

Advocates for strict privacy protections and supports international collaboration to address cross-border data challenges.

22. North Korea

Position:

North Korea maintains strict government control over digital communication. There is no transparency regarding data collection, and digital surveillance is used to monitor citizens and suppress dissent.

Stance on Regulation:

Opposes external regulation of domestic digital practices and rejects international oversight of state surveillance.

23. Cuba

Position:

Cuba enforces strict government control over digital communications through laws like Decree-Law 370, which regulates online content and allows heavy surveillance. Internet access is restricted, and digital privacy is limited.

Stance on Regulation:

Opposes international oversight of state surveillance and supports sovereign control over digital infrastructure.

24. Venezuela

Position:

Venezuela uses digital surveillance to monitor political opposition and restricts internet freedoms under the Law on Social Responsibility in Radio, Television, and Electronic Media. Data protection laws are underdeveloped, leaving citizens vulnerable to privacy violations.

Stance on Regulation:

Opposes external interference but may support regional cooperation to improve cybersecurity while maintaining state authority over digital monitoring.

25. Mexico

Position:

Mexico has established privacy frameworks under the Federal Law on the Protection of Personal Data but struggles with weak enforcement. Surveillance programs, like Pegasus spyware, have raised concerns over unlawful monitoring of journalists and activists.

Stance on Regulation:

Supports international cooperation to strengthen privacy protections but prioritizes national security concerns over full transparency.

26. Indonesia

Position:

Indonesia passed the Personal Data Protection Act (2022) to regulate personal data, but

enforcement remains inconsistent. The government retains broad surveillance powers under the Electronic Information and Transactions Law.

Stance on Regulation:

Supports international guidelines for digital privacy while maintaining the government's right to monitor digital activity for national security.

27. Ethiopia

Position:

Ethiopia lacks comprehensive privacy laws and has been criticized for mass digital surveillance under the Computer Crime Proclamation. State monitoring of social media and digital communications is common.

Stance on Regulation:

Opposes international oversight but may support regional initiatives aimed at improving digital infrastructure and cybersecurity.

28. South Africa

Position:

South Africa enforces the Protection of Personal Information Act (POPIA), promoting individual data rights while allowing limited state surveillance. It advocates for digital privacy and ethical data use.

Stance on Regulation:

Supports global data protection standards while encouraging corporate responsibility and international collaboration on cybersecurity.

29. Pakistan

Position:

Pakistan implements digital surveillance through the Prevention of Electronic Crimes Act (PECA), which allows the government to monitor and censor online activity. Data privacy frameworks remain weak and loosely enforced.

Stance on Regulation:

Supports national sovereignty over data and surveillance practices while being open to international cooperation for enhanced cybersecurity.

30. Nigeria

Position:

Nigeria enforces the Nigeria Data Protection Regulation (NDPR), but weak enforcement and government surveillance under the Cybercrimes Act remain concerns. The country faces rising cyber threats and privacy issues.

Stance on Regulation:

Supports enhancing data protection and international cooperation while prioritizing national control over digital surveillance for security purposes.

VII. References

Shea, S., & guide, s. (n.d.). What is Cybersecurity? Everything You Need to Know. TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/definition/cybersecurity

What is Data Privacy? (n.d.). SNIA. Retrieved from https://www.snia.org/education/what-is-data-privacy

What is Artificial Intelligence (AI) ? (n.d.). IBM. Retrieved from https://www.ibm.com/topics/artificial-intelligence

Cloudian. (2022, 20 de junio). Data Protection and Privacy: 12 Ways to Protect User Data. https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-wa%20ys-to-protect-user-data/

Cyber / online crime | The Crown Prosecution Service. (2022). https://www.cps.gov.uk/crime-info/cyber-online-crime

Personal Data Protection and Privacy | United Nations - CEB. (s. f.). https://unsceb.org/privacy-principles

Data Protection and Privacy Legislation Worldwide. UNCTAD. (n.d.). Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

1.2 billion euro fine for Facebook as a result of EDPB binding decision. (n.d.). Europa.Eu .Retrieved from

https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Bischoff, P. (2019, October 15). *Data privacy laws & government surveillance by country: Which countries best protect their citizens?* Comparitech. https://www.comparitech.com/blog/vpn-privacy/surveillance-states/

Data Protection and Privacy Legislation Worldwide. (n.d.). UN Trade and Development (UNCTAD). Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Data protection laws of the world. (n.d.). Dlapiperdataprotection.com. Retrieved from https://www.dlapiperdataprotection.com

What is a cyberattack? (n.d.). IBM. Retrieved from https://www.ibm.com/topics/cyber-attack

Kondruss, B. (n.d.). The terrifying list of cyber attacks worldwide 2024 / 2023 today. KonBriefing.com. Retrieved from https://konbriefing.com/en-topics/cyber-attacks.html