Online Safety Laws by Country

Haoming Song
Stanford University

Angie Holzer
WikiCharities

Follow this and additional works at: https://scholarsarchive.byu.edu/joni

Part of the Civic and Community Engagement Commons, International Relations Commons, and the Nonprofit Administration and Management Commons

Recommended Citation
Available at: https://scholarsarchive.byu.edu/joni/vol3/iss3/3

This Article is brought to you for free and open access by the Journals at BYU ScholarsArchive. It has been accepted for inclusion in Journal of Nonprofit Innovation by an authorized editor of BYU ScholarsArchive. For more information, please contact ellen_amatangelo@byu.edu.
Online Safety Laws by Country

By Haoming Song & Angie Holzer, EdD, JoNI Team

Overview: Statistics show that 493.33 million cyberattacks occurred on the internet last year alone, with a hacking incident taking effect once every 39 seconds. This surge of attacks has caused significant damage to the personal data that users circulate online, with data breaches averaging $4.35 million in losses in 2022. The rising new threat combined with its tremendous digital consequences have ignited countries around the world to draft new legislation to protect their citizens from online threats. This article examines a number of countries around the world by continent and highlights laws that they have put in place to protect their nation's data from being compromised.
Introduction

The 21st century is distinctively marked as a period of rapid technological development. An estimated 5.3 billion people around the world use the internet in some form, making up 65% of the world population, and that number is projected only to rise (Demand Sage, 2023). However, with the proliferation of technology also comes the introduction of new threats that have surfaced within our digital environment. Statistics show that 493.33 million cyber-attacks occurred on the internet last year alone (Techopedia, 2023), with a hacking incident taking effect once every 39 seconds (Astra, 2023). This surge of attacks have caused significant damage to the personal data that users circulate online, with data breaches that resulted in $4.35 million in losses in 2022 (Techopedia, 2023). These rising new threats combined with their tremendous digital consequences have ignited countries around the world to draft new legislation to protect their citizens from online threats. This article examines a number of countries around the world by continent and highlights laws that they have put in place to address these issues.

International Standards

The United Nations (UN) has taken many actions to protect people online. The United Nations is an international organization that was founded in 1945 for the purpose of maintaining international peace and security. Many of the UN’s agencies have been tasked to combat various online threats. These efforts include the United Nations International Children’s Emergency Fund’s (UNICEF) efforts to fight cyberbullying, the United Nations Educational, Scientific, and Cultural Organization’s (UNESCO) efforts to stop human trafficking, and the United Nations Office on Drug and Crime’s (UNODC) efforts to increase internet security, among many more agencies efforts and objectives. The UN and UNICEF have both also laid out the foundation for children’s rights through various policies and legislations, like the Convention on the Rights of the Child. Digital protection is included among these rights. The UN Committee on the Rights of the Child (CRC) has recommended that governments take swift action in the form of enacting policies to protect children from harm in the digital realm, stating that children “should also be protected from all forms of violence that happens in the digital...

![Figure 1. DLA Piper’s Data Protection Laws of the World (DLA Piper, 2023).](image-url)

**Europe**

Europe is one of the frontrunners in protecting their users online, in large part due to the efforts of the European Union (EU). The political union, consisting of 27 different European countries, passed the General Data Protection Regulation (GDPR) in 2018, laying the foundations for data protection and privacy in the EU. Under the GDPR, companies are obligated to follow strict regulations when processing user data, such as upholding data minimization, purpose limitation, and obtaining consent from the user. Data users were also given several rights over their own data, such as the right to complain, object, or request an erasure. This momentous legislation also provided special protections for children, requiring parental consent for users under the age of 13. The GDPR is considered as one of the most prominent and foundational pieces of legislation in the data protection movement. Many countries have subsequently adopted its policies, regulations and user rights, rehashing its content into their own legislations.

Some European countries outside the EU also have data protection laws. For example, Great Britain implemented the GDPR into their system through passing the Data Protection Act of 2018 (Gov.UK: The Data Protection Act, 2023). However, Russia has not passed any cybersecurity laws, and coverage of online data falls to older legislation, like personal data being protected under the Federal Law of 27 July 2006 (Data Guidance, 2022).

**United States**

Data protection in the United States is noticeably different from the European Union, in the fact that it technically does not contain a comprehensive nationwide data protection policy on the federal level. One of the only federal-level privacy laws in effect until recently, was the Privacy Act of 1974 that protects certain records of individuals, such as social security numbers, name, or other numbers or symbols dealing with personal identification, and prohibits agencies from disclosing them without user consent (U.S. Department of Health and Human Services, 2023). Much of the robust legislations regarding online data protection have been left to the states to draft. For example, California alone has 25 different laws in effect regarding personal data, like the California Consumer Privacy Act (CCPA), which formally states the personal rights of data users and imposes restrictions on processing data, similarly to the GDPR (DLA Piper, 2023).

One area in which the United States excels in comparison to other countries is extending additional specific legislation for the digital protection of children. The Children’s Online Personal Protection Act, passed in 1998, ensures the safety of minors under the age of 13 by giving parents the authority over what data websites can extract from their kids. Additionally, the act imposes further restrictions on what information can be taken from children online, and also provides a firm definition of parental consent (Federal Trade Commission, 2023). The US Congress recently followed up on this movement in 2023, introducing the Kids Online Safety Act. The bipartisan-supported bill doubles down on social media companies, requiring them to consider the safety of children through
implementing options on their platforms for children and parents to protect their data and performing security checks (Marsha Blackburn, 2023).

Central & South America
Websites suggest that online safety laws or regulations in Central and South America are missing or weak. Most of the countries listed by DLA Piper’s ‘Data Protection Laws of the World’ are judged to be “limited” or “moderate”. For example, Colombia does not have any laws in effect regarding online privacy (DLA Piper, 2023). However, efforts are still being made in many countries to provide their citizens with some form of online security, like Brazil’s General Data Protection Law (LGPD) (DataGuidance, 2023).

Mexico
Mexico has yet to implement a cybersecurity law, and although proposals have been issued by legislators to regulate private enterprises in various manners, none have officially gone through or been discussed. Mexico continues to struggle with cybersecurity and malware attacks, with over 85 billion cyber-attacks attempted in the first half of 2022 alone, more than 40% in frequency compared to the same period in 2021 (In-House Lawyer, 2023).

Argentina & Uruguay
Two of the countries in this region with the strongest data protections are Argentina and Uruguay. Article 43 of Argentina’s Federal Constitution states that any person may file for access to their personal data and request correction, suppression, or confidentiality in updating it. In addition to its Constitution, Argentina also passed the Personal Data Protection Law (PDPL). It is a comprehensive data protection law that regulates data processors and gives personal rights to data users in alignment with international standards and the GDPR (DLA Piper, 2022). Uruguay’s data protection law, known officially as Data Protection Act 18331, establishes the Personal Data Regulatory and Control Unit (URCDP) as a data supervisor and regulates the use of “personal data”, which is broadly defined as data related to individuals and legal entities. The legislation also implements stricter protections of “sensitive data,” which refers to certain content like sex life, racial or ethnic information, public health, and other subjects (ITechLaw, 2023).

Africa
Many countries in Africa have recently passed their own national legislation cementing regarding data protection. As of February 2023, 36 out of 54 countries in Africa have implemented laws of some sort regarding data security. Many of these laws share commonalities with the European Union’s GDPR, like the same basic data user rights and also the same regulations towards data processors like purpose limitation and data minimization.

Some examples of more recent legislation passed regarding online safety in Africa include the Eswatini Data Protection Act in 2022, outlining similar regulations and personal rights as the GDPR, and including the requirement for explicit verbal consent by the individual with set guidelines on what constitutes consent. Tanzania’s Personal Protection Act, passed in 2022, also contains data processing rules and personal data rights that are covered by the GDPR. They also revised the Electronic Transactions Act in the same year, which doubled down on regulating the processing of electronic transactions, obligating senders to send a restricted amount of content and requiring consent from the receiver to go through, along with giving them a free option to opt out of the deal. Uganda recently passed the Computer Misuse Amendment Act in 2022, which prohibits sending of “unsolicited information”, which is broadly defined as “information transmitted to a person using the internet without the person’s consent” (Lexology, 2023).
Another highlight of Uganda’s legislation is its focus on child safety in particular, prohibiting the sharing of children’s data without authorization from their parents or guardians. Besides Uganda, a couple of other countries in Africa have also made efforts at specifically making the online environment safer for minors. Nigeria’s Child Rights Act distinctly states that children have the right to privacy, including on the internet, while their Cybercrimes Act, passed in 2015, institutes strict punishments on the production of pornography and film (Source). Another example of a country with specific legislation towards online child safety is Rwanda. The Rwanda Child Protection Policy, also deemed “the COP Policy”, lists out an intricate framework that the Rwandan government plans to take to ensure the digital protection of its minors, including implementing special categories for the regulation of children’s data, expanding the investigation, prosecution, and sentencing for child online sexual abuse, establishing a response system against online child abuse, and employing a committee to make sure that such rules and regulations are firmly implemented.

Asia

Many countries in Asia have passed national cybersecurity bills, monitoring the protection of citizens’ personal data, such as Japan’s Act on the Protection of Personal Information (APPI) (Didomi, 2023), the Phillipines’s Data Privacy Act of 2012 (National Privacy Commission, 2023), and South Korea’s Personal Information Protection Act (DataGuidance, 2023). Indonesia passed their first data protection law in 2022 with the Personal Data Protection Bill (Thales, 2023), and Vietnam also passed its first law regarding this topic with Decree No. 13 on the Protection of Personal Data (Squire Patton Boggs, 2023).

China

China has taken major steps towards online safety, passing three pieces of legislation that make up the core of its data protection and cybersecurity framework. The 2016 Cybersecurity Law (CSL), the first of the three passed and the first ever cybersecurity law enacted in the country, created a regime known as the Multi-Layer Protection Scheme to oversee the construction, operation, maintenance, and use of networks in the country. The second and third pieces were both passed in 2021, known as the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). The former announced the emphasis of “data security” from a national perspective, although the term is broadly defined in the legislation. The latter makes up China’s privacy law, with resemblance to the GDPR in the EU (Source). China is also a standout when it comes to the data protection of children. The PIPL classifies the personal information of children under 14 as “sensitive,” and requires data processors to obtain parental consent before processing their data (Oxford Academic, 2023). More importantly, the country issued the Provisions on Online Protection of Children’s Personal Information in 2019, restressing the requirement of parental consent prior to the manipulation of children’s personal information, with strict regulations on what network operators must provide to legally obtain that consent (Library of Congress, 2019).

India

India recently revised their legislation by passing a long-due revision of the Digital Personal Data Protection Act in early August of 2023. It establishes grounds for the collection and processing of personal data. Consent is required, and it must be “freely given,” “specific,” “informed,” “unconditional,” an “unambiguous indication of consent” through a “clear affirmative action,” and be able to be withdrawn at any time. However, the act also states that consent may not be required for “legitimate uses”, such as for public health matters, compliance with the court, or during a medical emergency. A notice must be given by data processors to the clients before processing their data. Data fiduciaries are required to ensure that personal data is safely protected or erased when needed to prevent a...
data breach, and in the event of such an event occurring, must inform the Data Protection Board of India under the government. Finally, the legislation contains a section designated to protect the data of children under 18, requiring parental consent and prohibiting targeted advertising towards children. The Act is set to take effect ten months after its passing, but no specific date has yet to be defined (Hunton Andrews Kurth, 2023).

**Saudi Arabia**

Saudi Arabia stands out in terms of its data protection for children specifically. Their legislation, the Children and Incompetencies’ Privacy Protection Policy, contains many protection guidelines for children’s data, with clear and concise definitions and procedures listed in the document (National Data Management Office, 2020). The specificity of the legislation has earned Saudi Arabia the position of being one of the safest countries in the world for children’s data (Comparitech, 2023).

**Australia**

Australia has a vast system of data protection and cybersecurity laws. Main data privacy protection comes in the form of the Privacy Act, enacted in 1988, which regulates the handling of all personal information by business and private entities. Such regulations expand and apply to personal information found online (DLA Piper). The Security of Critical Infrastructure Act was passed in 2018 to monitor national security and prevent risks like sabotage, espionage, and coercion, and also requires entities under the law to report cybersecurity incidents to the government (International Comparative Legal Guides, 2023).

One weakness of Australia’s robust amount of online data security legislation is a lack of specification to children’s data, which is treated and regulated in the same manner as that of adults (Comparitech).

**Conclusion**

Countries around the world have been making admirable strides towards protecting their citizens online. Representative institutions such as the European Union have paved the way for cybersecurity legislation across the world, and many countries have followed suit enacting laws modeled after the GDPR or have developed nationwide data protection or privacy legislation of their own. However, while many countries around the world have been making adamant strides to create laws, there still exists room for improvement. For example, some countries’ laws allow governments to directly bypass the regulations under certain circumstances. Although this may be desirable in cases such as national security, it can also provide unwanted loopholes contrary to the intent of the law for predatory government action, corrupt government actors, or even commercial or other entities to access data. (Comparitech, 2023). There are also regions, such as Central and South America, where cybersecurity laws are considerably weak or nonexistent. These nations need to do more to protect their citizens from harm online. As online threats continue to be rampant in a rising era of technology, countries need to make sure that they have the laws and regulations in place to combat them.

**References**


2ee-10bd-4eb9-a614-a990c236bb45


