Scientific Research Publishing

Open Journal of Social Sciences, 2025, 13(9), 590-610
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

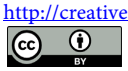
A Comparative Study of Cybersecurity Responses in China, South Africa, Nigeria, and Zimbabwe to Cybercrimes against Young Women and Children

Lindsay Thobekile Bria Lunga, Fei Tang*

School of Law, Yangtze University, Jinzhou, China
Email: lindsaylunga@yahoo.com, *tangfei928@163.com

How to cite this paper: Lunga, L. T. B., & Tang, F. (2025). A Comparative Study of Cybersecurity Responses in China, South Africa, Nigeria, and Zimbabwe to Cybercrimes against Young Women and Children. *Open Journal of Social Sciences, 13,* 590-610.
https://doi.org/10.4236/jss.2025.139036

Received: August 18, 2025
Accepted: September 25, 2025
Published: September 28, 2025



Abstract

The World Wide Web has changed the way individuals communicate, the tools used to learn, and almost over 60 percent have become users of the internet. On the other hand, the internet has many hidden dangers to which young women and children have been exposed, such as online harassment, cyberbullying, grooming, exploitation, and revenge porn. This paper is a comparison between China and African countries such as South Africa, Nigeria, and Zimbabwe on their responses to cyber-threats in their jurisdictions. The study uses a comparative legal research method to examine the differences and similarities in cybersecurity laws in the mentioned countries, and deterrence theory was used to help explain the laws and enforcement. This paper highlights the most common cybercrimes affecting young women and children and the specific laws that protect them.

Keywords

Cybercrime against Women and Children, Comparative Cybersecurity Law, Online Child Protection, Deterrence Theory in Cyber Law

1. Introduction

There are several misconceptions surrounding the phrase "laws that govern the internet," often associating it solely with government control and censorship. Such laws are essential for regulating online spaces and protecting users from cybercrimes, as many offenders exploit the anonymity provided by the internet to commit crimes that often begin online and later escalate into physical harm. With

*Corresponding author.

the rapid growth of internet use and advancing technology, young women and children have become particularly vulnerable to a range of internet-facilitated crimes. Today, the internet is integral to daily life, with increasing accessibility allowing even children as young as eight to engage online, making the need for both national and international legal frameworks to ensure safer internet use increasingly urgent. This paper examines crimes such as harassment, cyber-bullying, online child exploitation, cyber-pornography, and cyber-stalking, with a focus on legal protections for young women and children, and compares the effectiveness of laws in the People's Republic of China, South Africa, Nigeria, and Zimbabwe. Recently reviewed work highlights progress and numerous constraints concerning the enforcement of cyber security laws in Africa: Matsaung and Masiloane (2024) note that cyber-intelligence practices may increase investigative capacity but are weakened by a lack of skills, unavailability of equipment, and divisions among government agencies (African Security Review), while Ngece, Mkhize, and Majola's qualitative study of the South African Police Service identifies capacity and resource limitations, incomplete procedures, lack of training, and inability to respond effectively to cybercrimes, though recommending specialized units and stronger inter-agency collaboration (Ngcece et al., 2025).

2. Definitions

According to Kahn and Cerf (1999), the internet is a vast global network connecting computers worldwide, enabling access to information and global communication. While the internet is used for various purposes such as banking, research, and investment, its most common uses are entertainment and socializing. It is largely owned and managed by private companies that control much of the content uploaded and recognize how deep and difficult it is to regulate. Lindsey (2020) defines young women as females in the transitional stage of adulthood, generally ranging from ages 18 to 35, though definitions may vary by country. The United Nations General Assembly Convention on the Rights of the Child (United Nations General Assembly, 1989) defines children as individuals under the age of 18, emphasizing their developmental stage and limited capacity for self-preservation. Bucy (2000) states that both young women and children have broad access to the internet, making them highly vulnerable to anonymous individuals with malicious intent. While all internet users face risks, these two groups are often considered the most at risk.

Datareportal Global Digital Insights (2024) reports that over 5 billion people, more than 60% of the global population, now use the internet. Given the scale and the potential dangers, cybersecurity laws have become important to protect young women and children from crimes committed online. Their safety can be ensured using legal structures that address their unique vulnerabilities in the digital space. According to Greiman (2022), cyber law, also known as internet or digital law, encompasses legal frameworks that govern digital activities. It includes regulations to prevent cybercrimes, protect personal data, and guide online conduct.

These laws cover a broad spectrum of issues, such as privacy, intellectual property, cybersecurity, and freedom of expression in the digital realm. Kamble (2013) explains that cyber laws aim to deter digital crimes, safeguard internet users, and protect digital assets. Cybercrime involves a wide range of illegal activities conducted through computers and networks; these may include crimes such as harassment, cyber-bullying, online child exploitation, cyber-pornography, and cyberstalking, just to mention a few.

Cyberstalking involves persistent, unwanted attention and harassment through digital means, and may include death and humiliation. Faith (2022) highlights that victims often struggle to recognize the seriousness of these acts and their lasting emotional, psychological, and financial effects. Jane (2020) notes that social media platforms have become breeding grounds for this harassment, where young women endure body shaming, public humiliation, and unsolicited explicit content. Severe cases, such as Amanda Todd's, as documented by Butt (2024), demonstrate how relentless online stalking and image-based abuse can escalate to tragic outcomes like suicide.

Online Grooming occurs when offenders, often posing as peers, befriend and manipulate children online, gaining their trust to exploit them emotionally or sexually. Ateş, Bostancı and Güzel (2018) identify popular platforms like Roblox, Minecraft, and Fortnite as frequent grooming venues. Predators exploit anonymity and children's limited digital literacy to solicit explicit images or personal details. The Amanda Todd case also exemplifies this, where the perpetrator groomed Amanda before distributing her images, triggering prolonged abuse (Butt, 2024).

Online harassment includes a wide spectrum of aggressive digital behaviour, from sexist jokes and hate speech to explicit threats and identity theft. Shekhawat (2022) underscores the financial and emotional damage victims endure from such abuse. Stoilova, Livingstone, and Khazbak (2021) highlight how exposure to harmful content and misinformation desensitizes youth to violence and fosters unhealthy attitudes. Jane (2020) further reports that sexual harassment, body shaming, and gender-based slurs are common on social media, causing victims severe psychological distress, including anxiety, depression, and self-harm risks.

3. Methods

Tomlinson (2016) asserts that deterrence theory holds that criminal penalties not only serve to punish offenders but also deter others from committing similar crimes. The deterrence theory informed that effective implementation of cybersecurity laws can reduce offenses by discouraging potential violators. Legislative texts such as the cybersecurity laws of each country and secondary sources such as academic articles, reports, and case studies were used in this study. Shackelford (2016) further emphasizes that states have a duty to align domestic legislation with international human rights conventions, such as the Convention on the Rights of the Child and CEDAW, to protect women and children from online violence and exploitation. Addressing the global nature of cybercrime, Sharma (2023) high-

lights the importance of international cooperation and partnerships with private entities, while Harkin and Whelan (2022) underline the need for specialized police training and a judiciary equipped to handle cyber-related cases sensitively and effectively. To meaningfully assess the adequacy of these protective frameworks, a comparative legal research method is essential. It enables a systematic examination of the similarities and differences in cybersecurity laws between China and African countries like South Africa, Nigeria, and Zimbabwe. The African countries were selected on the basis of sharing a colonial background, and all were banded together by their levels of internet penetration. The comparative legal research method helps identify legal gaps, effective enforcement strategies, and culturally appropriate reforms, ensuring improved protection for vulnerable groups within diverse digital environments.

4. Results and Discussions

China's Cyber Law

According to Chiu (1985), the 1982 Constitution, still in effect today, laid the foundation for legal and economic reforms. China has developed a complex legal system with influences from civil law traditions, Germany, Japan, and socialist legal principles while ensuring the Communist Party retains ultimate authority. The Cybersecurity Law of the People's Republic of China of 2016 (National People's Congress of China, 2016), Protection of Citizens and Minors, Article 12, ensures citizens' rights to network access while prohibiting activities that endanger national security, disrupt social order, or infringe on individuals' rights. Article 13 mandates state support for the development of online services that benefit minors and criminalizes harmful online activities targeting children. Articles 40-44 impose strict data protection measures on network operators. They must maintain user confidentiality, collect and use data lawfully, and obtain user consent. They are prohibited from disclosing or tampering with personal data unless personal information has been redacted or legally required. Individuals have the right to request deletion or correction of their data if collected unlawfully or contains errors. Articles 47-50 require network operators to manage user-published content and remove prohibited information. Authorities that oversee cybersecurity can block or remove harmful content from foreign sources. Article 64 enforces penalties for breaching data protection laws, including fines of up to RMB 1,000,000, confiscation of unlawful gains, and business suspensions. Unauthorized access, sale, or misuse of personal data may result in severe fines and criminal prosecution. These laws may be used along with the Personal Information Protection Law of 2021, and the Law on the Protection of Minors of 1991 to bring the perpetrators of cybercrimes to justice. By making the laws specific, this helps deter future perpetrators of cybercrime in China; this concurs with the deterrence theory.

Xinhua (2024) reports that there are over a billion internet users in the People's Republic of China, meaning that more than 70% of the population maintains a digital footprint. In response to the growing risks associated with widespread in-

ternet access, China has established cyber laws with specific provisions aimed at protecting minors. Notably, the Public Security Administration Punishment Law stipulates that individuals who use the internet to harm minors or disseminate harmful information will face severe penalties. In addition to legislative measures, the government has actively collaborated with organizations such as Plan International to enhance online safety. According to Plan International (2022), this partnership has led to the launch of several nationwide campaigns designed to educate young people about the dangers of the internet and ways to safeguard themselves. These initiatives focus on helping minors recognize and avoid online predators, use social media responsibly, and report any instances of cybercrime they may encounter.

China has taken proactive steps by forming bilateral agreements to enhance international collaboration in cybercrime investigations (Ma, 2024). Collaborative efforts with organizations like the China Internet Network Information Centre and non-profits such as the Anti-Cyberbullying Alliance have fostered public awareness campaigns, educating families about online safety measures and reporting mechanisms (China Internet Network Information Center (CNNIC), 2024). The Cyber Security Law of 2017 provides a legal framework that facilitates cooperation among law enforcement, educational institutions, and tech companies to strengthen protective measures. China's judicial system has enhanced enforcement, and specialized cybercrime units have been established within law enforcement agencies, focusing on detecting and prosecuting offenses such as online harassment, exploitation, and trafficking. According to Pyo (2021), the Supreme People's Court has also played a crucial role by issuing judicial interpretations that provide clearer guidelines for handling cybercrime cases involving vulnerable groups. These interpretations assist judges in applying relevant laws consistently and effectively. Public awareness campaigns have been launched to educate citizens about the dangers of cybercrime and the importance of online safety. This includes the service of sending messages to mobile numbers, reminding users not to answer calls from unknown numbers or click on messages that have also been sent by unknown numbers.

According to Cuihong (2018), government agencies in China are encouraged to work collaboratively with non-governmental organizations and the private sector to foster a safer online environment. The implementation of cyber laws has also facilitated international cooperation in addressing cybercrimes. To strengthen online safety, China has introduced several key regulations, including the Personal Information Protection Law, which prevents unauthorized access, breaches, and personal data loss, the Data Security Law, which regulates the storage and transfer of personal data, and the Internet Service Administration Law, which regulates the data on online platforms. These laws require network operators to adopt necessary measures to safeguard personal information and prevent the dissemination of illegal or harmful content (Wang, Hsieh, Chang, Jiang, & Dallier, 2021).

Social media platforms used within the country have been urged to adopt stricter monitoring and reporting protocols, bolstering their roles in protecting vulnerable users as alluded to in an article by South China Morning Post (2023). However, despite these legislative advancements, online abuse remains a persistent challenge. A tragic example is the case of Zhen Linghua, a 23-year-old woman who became the target of relentless cyberbullying after posting a photo celebrating a personal achievement with pink-dyed hair. Anonymous users labelled her a "pink hair prostitute" and spread malicious rumors about her relationship with her grandfather. The sustained harassment lasted for six months and resulted in her suicide (Lu, 2023). This incident underscores the gaps in enforcement and the insufficient protection for vulnerable groups, particularly young women. Although China has made notable progress in cyber legislation, its governance continues to prioritize economic and national security interests over individual rights. Greater focus is needed on protecting freedom of expression and ensuring that online platforms, law enforcement, and judicial systems effectively address harassment and abuse in digital spaces.

South Africa's Cyber Law

The Republic of South Africa is a constitutional state, with a supreme Constitution and a Bill of Rights. South Africa has a mixed legal system which is a hybrid of Roman Dutch civilian law, English common law, customary law, and religious personal law according to van Niekerk (1998). The South African Cybercrimes Act 19 of 2020 (Government of South Africa, 2021) outlines various offenses and penalties related to cyber-related crimes, emphasizing the protection of personal data and digital security. Article 7 criminalizes the unauthorized acquisition, possession, or distribution of passwords, access codes, and biometric data for illicit purposes. Article 10 defines cyber extortion, where individuals unlawfully commit or threaten cyber offenses to gain an advantage or force compliance. Article 11 introduces aggravated offenses, targeting cybercrimes against financial institutions and government systems, as well as cyber activities that endanger lives, public safety, or create emergencies. Articles 14 and 15 criminalize electronic threats, including incitement to violence and property damage through data messages. Article 16 prohibits the non-consensual distribution of intimate images, protecting individuals from online sexual exploitation and privacy violations. Article 19 sets penalties for various offenses, including imprisonment of up to 15 years for severe violations. Article 20 introduces protection orders, allowing victims of cyber harassment, threats, or image-based abuse to request court orders to prevent further dissemination of harmful content. Article 54 requires electronic service providers and financial institutions to report cybercrimes within 72 hours to law enforcement and preserve relevant evidence, with non-compliance resulting in fines up to R50,000. Article 55 mandates the establishment of cybercrime detection, prevention, and investigation units within the South African Police Service (SAPS), ensuring officers receive specialized training. The following are laws that can be used along with the Cybercrimes Act: Electronic Communications and

Transactions Act (2002) [Act No. 25 of 2002], Protection of Personal Information Act (2013) [Act No. 4 of 2013], Regulation of Interception of Communications and Provision of Communication-Related Information Act (2002) [Act No. 70 of 2002], Prevention of Organised Crime Act (1998) [Act No. 121 of 1998], Films and Publications Act (1996) [Act No. 65 of 1996] (as amended in 2019), and the Children's Act No. 38 of 2005.

In Africa, there are more than 570 million internet users. The numbers are low due to the high cost of using the internet, as stated in an article by Galal (2024). According to an article by Cowling (2024), there are an estimated 45 million people who use the internet in South Africa, and this estimate comprises more than 70% of the total population. In South Africa, where cybercrimes against women and children are on the rise, the implementation of cyber laws has become crucial in ensuring their safety and justice. According to Smit (2024), cyber laws in South Africa, such as the Electronic Communications and Transactions Act and the Protection from Harassment Act, have been specifically designed to safeguard individuals from online harassment, cyberbullying, and other forms of digital abuse.

In South Africa, a Cyber Crime Unit was established within the South African Police Service, and this enabled specialized investigations into incidents such as online grooming, sexual extortion, and cyberbullying according to Modise (2025). According to an article by Masiphephe Network (2023) about cybercrime in South Africa, partnerships with organizations such as Childline South Africa and the South African Depression and Anxiety Group have provided support systems for victims and promoted awareness. The Cyber Crimes Act has strengthened the legal framework for prosecuting cyber offenses, facilitating collaboration between law enforcement and internet service providers to improve reporting mechanisms promoting general deterrence on a larger scope of the public. Cooperation between international law enforcement agencies is essential but often complicated due to bureaucracy. According to the South African Police Service (2015, June 17), such cooperation enabled South Africa to apprehend a cybercriminal involved in a global child pornography network. A tip-off from Belgian police led to his conviction and a 15-year prison sentence. These partnerships have proven effective in tracking and prosecuting cross-border offenders. Strengthened international cooperation remains crucial in addressing cybercrime globally.

According to Mokofe (2023), the judiciary system has been conducting specialized training programs for criminal justice practitioners. These programs aim to develop and clarify perspectives on gender-based violence, specifically in the context of cyber violence against women and girls. They provide background information on international and regional standards and legislation on gender-based violence and cybercrime, and discuss cybercrime instruments. According to Powell & Schonwetter (2019), the African Commission on Human and Peoples' Rights has called on states, including South Africa, to review and adopt legislation that combats all forms of digital violence. This includes expanding the definition of gender-based violence to encompass digital violence against women, such as

cyber-harassment and cyberstalking. According to an article by the South African Government (2023), the Film and Publication Board focuses on educating parents and children about the risks in digital spaces.

According to Snail ka Mtuze and Musoni (2023), the implementation of cyber laws has enabled prosecutors to effectively charge and convict individuals involved in the online exploitation of women and children. Cyber laws supported by awareness campaigns aim to educate users on the risks of sharing personal information, the importance of privacy settings, and how to report cybercrimes. To promote internet safety in schools, the Department of Basic Education, in collaboration with the Western Cape Education Department and Google, hosted an Online Safety Curriculum Guideline Strategic Workshop. This initiative targeted national and provincial education officials involved in Life Orientation, School Safety, E-Learning, and Quality Learning and Teaching Campaign programs. The resulting Online Safety Curriculum for Grades 8 - 12 is designed to support Life Orientation teaching and ensure learners, teachers, and parents understand how to stay safe online (Department of Basic Education, Republic of South Africa, 2024). When this specific group of vulnerable individuals learns about the importance of cyber safety, they also learn about the penalties for the crimes, thus deterring cybercrime. Despite these efforts, many South Africans remain victims of cybercrime, often choosing not to report incidents due to limited police capacity. According to Modise (2025), law enforcement faces shortages in human resources and technical expertise, hindering their ability to address cybercrimes effectively. As cybercrime continues to rise, ordinary users are increasingly at risk of personal data breaches. While the government has made strides in protecting national interests and state secrets, ordinary citizens still lack the same level of cyber security protection.

Nigeria's Cyber Laws

In Nigeria, the Constitution is the supreme law of the country, and there are four distinct legal systems: English law, Common law, customary law, and Sharia law. English law in Nigeria was inherited from the colonial era, while Common law developed after the country's post-colonial independence (Nwosu, 2015). The Nigeria Cybercrimes Act of 2015 outlines various offenses, penalties, and protective measures concerning cyber-related crimes. Article 6 criminalizes unauthorized access to computer systems for fraudulent purposes, imposing penalties of up to 7 years' imprisonment or fines of N7,000,000.00 for offenses involving classified information. Article 22 targets the fraudulent issuance of electronic instructions within financial institutions, penalizing offenders with 7 years of imprisonment. Article 23 addresses child pornography, criminalizing its production, distribution, possession, and solicitation with penalties of up to 15 years' imprisonment and fines of N25,000,000.00. Article 24 defines cyberstalking, making it illegal to send offensive, threatening, or misleading messages via digital platforms, with penalties reaching 10 years' imprisonment and fines up to N25,000,000.00. Article 26 criminalizes racist and xenophobic offenses, including distributing material that in-

cites hatred or denies crimes against humanity, punishable by 5 years' imprisonment or fines up to N10,000,000.00. Article 29 imposes penalties on service providers who misuse consumer data for fraudulent financial gain, leading to fines of N5,000,000.00 or corporate forfeiture. Article 39 allows law enforcement to intercept and monitor electronic communications if required for a criminal investigation. Article 40 mandates that convicted offenders pay restitution to victims, covering financial losses or returning stolen assets. Institutions must report cyber threats to the National Cybersecurity Emergency Response Team (Article 22), with non-compliance leading to a N2,000,000.00 fine. The following laws are also used when prosecuting cybercrimes in Nigeria: the Criminal Procedure Act (1977) [Act No. 51 of 1977], Electronic Communications and Transactions Act (2002) [Act No. 25 of 2002], Protection of Personal Information Act (2013) [Act No. 4 of 2013], Regulation of Interception of Communications and Provision of Communication-Related Information Act (2002) [Act No. 70 of 2002], Prevention of Organised Crime Act (1998) [Act No. 121 of 1998], Financial Intelligence Centre Act (2001) [Act No. 38 of 2001], Copyright Act (1978) [Act No. 98 of 1978] (as amended), Films and Publications Act (1996) [Act No. 65 of 1996] (as amended in 2019), and the Children's Act (2005) [Act No. 38 of 2005].

In recent years, the rise of technology and the internet has brought about numerous benefits to society in terms of communication and access to information, with over 100 million internet users in Nigeria according to a report by Kemp (2024a). These advancements have also brought potential dangers for vulnerable groups such as young women and children. To mitigate these risks, the Nigerian government implemented cyber laws that aim to protect the rights and well-being of these groups. According to an article by Unit, I. C. T. Cybercrime and Cyber Law in Nigeria (2023), with the rise of social media and other online platforms, children are becoming increasingly vulnerable to sexual predators. Cyber laws in Nigeria have provisions that safeguard the privacy and confidentiality of individuals, especially minors. This ensures that their personal information is not exploited by others, which could potentially put them in harm's way.

The Nigerian government established the Nigerian Cybercrime Unit within the Economic and Financial Crimes Commission. It has been pivotal in addressing cyber offenses such as online harassment, exploitation, and trafficking. According to Nayak and Bello (2024), collaborations with organizations like the National Agency for the Prohibition of Trafficking in Persons and international bodies such as INTERPOL have bolstered efforts to investigate and prosecute offenders effectively. Non-governmental organizations are contributing to the fight, like the Nigerian Internet Safety Initiative, which focuses on raising awareness among young people and their families about online dangers, the importance of digital literacy, and the punishment for those that commit the crime to discourage deviant behavior. According to Ibekwe (2015), the enactment of the Cybercrimes Act in 2015 marked a pivotal development, criminalizing offenses such as cyberstalking, cyberbullying, and the distribution of child pornography.

The judiciary has undergone training to effectively interpret and apply cybercrime laws, ensuring that perpetrators are held accountable as stated by Obidimma and Ishiguzo (2023). There is encouragement of collaborative efforts among government agencies, non-governmental organizations, and the private sector to create a safer online environment. Cyber laws in Nigeria stipulate punishable offenses, providing legal protection to victims and deterring potential stalkers. For example, the case of a woman in Nigeria who was murdered after she was invited to a business meeting by people she met online. According to an article published by Vanguard.com (2017), she was befriended by two criminals on an online platform, she was stalked, robbed, raped, and murdered during her trip, and the criminals were then charged and received the death sentence. With the threat of legal consequences, individuals are more likely to think twice before engaging in cyberbullying, harassment, or other illegal activities. This, in turn, contributes to creating a safer and more positive online community for everyone, including vulnerable groups. However, the government treats cyber laws and cybercrimes as if they are a non-existent and invisible problem without considering that Nigeria has become a breeding ground for cybercrime.

Zimbabwe's Cyber Law

The Constitution is the supreme law of the Democratic Republic of Zimbabwe. Zimbabwe's legal system consists of Common law, non-statutory or unwritten Anglo-Roman Dutch Law, Legislation, Case Law, and Customary Law. Except for Criminal Law, which has recently been reformed and codified, Zimbabwe's law is not codified according to Madhuku (2010). The Zimbabwean Cybersecurity and Data Protection Act (Parliament of Zimbabwe, 2021) establishes safeguards for personal data, digital security, and online safety, particularly for women and children. Article 7 mandates data controllers to process information lawfully, ensuring accuracy and limiting retention periods. Article 13 requires transparency in processing personal data, ensuring privacy and fairness. Article 14 grants data subjects' rights to access, correct, or delete false personal information. Article 18 enforces security measures to prevent unauthorized access, while Article 19 mandates reporting of security breaches within 24 hours. Article 25 protects individuals from decisions based on automated data processing, while Article 26 ensures children's data rights are exercised by guardians. Article 28 regulates international data transfers, requiring adequate protection. To combat cyber offenses, Article 164A criminalizes sending threatening messages, imposing fines or up to five years' imprisonment. Article 164B addresses cyberbullying and harassment, punishable by up to ten years. Article 164C criminalizes false data transmission causing harm. Article 164E prohibits non-consensual distribution of intimate images, imposing five-year sentences. Article 164G penalizes identity-related offenses, including impersonation, with harsher penalties if minors are involved. Article 165 criminalizes recording beneath clothing without consent, like Article 164E, which covers unauthorized distribution of such content. For child protection, Article 165A criminalizes child sexual abuse material, imposing ten-year sentences for

production, distribution, or possession. Article 165B prohibits exposing children to pornography, penalizing offenders with up to five years. Additionally, adults engaging in online child grooming for sexual activities face up to ten years in prison. The following laws are used together with the Cyber and Data Protection Act (2021) to prosecute cybercriminals: Interception of Communications Act (2007), and Data Protection Regulations under the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) Act (2000).

Cyber-security has become an increasingly important concern in today's rapidly advancing digital world, with the number of internet users in Zimbabwe estimated to have surpassed 5 million (Kemp, 2024b). In response to rising cyber threats, the Computer Crime and Cybercrime Bill was signed into law in 2017, criminalizing offenses such as cyber-bullying, cyber-stalking, and other forms of online harassment. According to Chipfumbu, Tsokota, and Marovah (2024), the Cybercrime and Cyber-security Ministry, established in 2019, is tasked with developing and implementing strategies to prevent cyber threats and maintain a secure digital environment. Additionally, the Data Protection Act, enacted in 2019, mandates that personal data collected and stored by businesses and organizations be securely managed and used solely for its intended purpose. This legislation plays a crucial role in protecting vulnerable individuals from data breaches and identity theft, which can lead to profound consequences both online and offline.

The establishment of the Cyber Crime Unit within the Zimbabwe Republic Police has enhanced their ability to investigate and prosecute cases related to online harassment, child exploitation, and grooming. According to Poshai, Chilunjika, and Intauno (2023), the police have partnered with the Zimbabwe Child Protection Fund, and various NGOs have played a vital role in raising awareness about the risks of cybercrime and providing educational resources to families and communities. This also helps to deter individuals who are interested in committing cybercrimes within the communities. The implementation of the Computer Crimes and Cyber Crime Bill has strengthened legal frameworks, allowing law enforcement to address cyber offenses more effectively. Efforts by international organizations, such as UNICEF, have also contributed by promoting digital safety initiatives aimed at empowering young people. According to an article published by The Herald (2024), the Zimbabwe Republic Police hosted a debrief meeting for the Africa Cyber Surge Operation in Harare. The event brought together senior law enforcement officials and cybercrime experts from Interpol, the Southern Africa Regional Chiefs Co-operation Organization, and the African Union Mechanism for Police Co-operation. This was a meeting to foster relationships with various cybercrime organizations to promote cooperation, and computers were donated to the police department that deals with cybercrimes.

The enactment of the Cyber and Data Protection Act in 2021 marked a pivotal development, aiming to enhance cyber security and data protection. To bolster enforcement, the Act designates the Postal and Telecommunications Regulatory Authority of Zimbabwe as the Data Protection Authority, responsible for oversee-

ing compliance and ensuring the lawful processing of data. The judiciary has been empowered to interpret and apply cybercrime laws effectively, ensuring that perpetrators are held accountable and prevented from re-offending. Poshai, Chilunjika, and Intauno (2023) stated that the implementation of cyber laws in Zimbabwe has also led to the establishment of the Zimbabwe Cybercrime Online Reporting Network, which is an avenue that allows individuals to report cyber-related offenses, seek advice, and get assistance in cases of cyber abuse. According to an article by Bofu-Matinha (2024), the Ministry of Information Communication Technology and Postal Courier Services actively promotes cyber security awareness among citizens, and it organizes events during the National Cyber Security Awareness Month to educate the public on safe online practices and the risks associated with cyber threats. The ministry also collaborates with the Postal and Telecommunications Regulatory Authority of Zimbabwe and the International Telecommunications Union and has set up a National Computer Incident Response Team. This team serves as the crucial point for reporting and responding to cyber incidents. Despite these efforts, Chingoriwo (2022) argues that victims often refrain from reporting cybercrimes to the police due to numerous factors, including cultural norms and the fear of societal shame, particularly in cases involving young women and children.

The laws in Zimbabwe were put in place about five years ago, and the country has been unable to cope with the changing and developing technology. The implementation of these laws and acts requires a large movement of human resources that are well versed in technology to handle the reports and conduct the investigations. According to Mugari, Kunambura, Obioha and Gopo (2023), this entire process also requires large sums of money to implement, and with the current economic situation, the government is unable to facilitate the adequate implementation and enforcement of the law. Mugari (2020) argues that often these crimes move from the internet and take up a physical form, which becomes a dangerous situation, and if one does decide to report to the police, if there is no physical harm, then there is nothing they can do, and this leads to serious harm. The cyber security laws are also viewed as a means to control citizens and violate the citizens' rights to privacy and free speech.

Difficulties in investigating cybercrimes.

According to Savaş and Karataş (2022), it is crucial for states to manage internet usage not to control the flow of information, but to protect individuals from cybercriminals. A significant challenge arises from the fact that most countries do not own the servers hosting their citizens' data, as these are often managed by private companies, which can cause investigations to reach dead ends. Countries like Zimbabwe and Nigeria face additional difficulties due to limited resources and infrastructure, making it challenging to conduct large-scale cybercrime investigations. Proulx (2022) notes that cybercriminals frequently use tools such as virtual private networks, anonymizing software, and encryption to conceal their identities, complicating law enforcement efforts to trace their activities and deter-

mine the origin of cybercrimes. As a result, crimes committed through online platforms often go unresolved. In contrast, the People's Republic of China maintains control over its domestic servers, which, according to Liu (2021), offers the government greater capacity to track and manage internet activities. Nevertheless, the sheer volume of data generated online poses a further challenge, as investigators must navigate massive datasets, a process that Horan and Saiedian (2021) describe as both time-consuming and resource-intensive.

Similarities of the Four Countries

China, South Africa, Nigeria, and Zimbabwe share key similarities in their cybersecurity frameworks. First, all have introduced data protection and privacy laws, collaborating with domestic network providers and restricting the export of locally collected data. Second, each country has enacted cybercrime legislation addressing offenses such as child trafficking, identity theft, and child pornography, with specific laws ensuring that offenders can be properly charged (Bechara & Schuch, 2021; Deora & Chudasama, 2021). Third, they have developed national cybersecurity strategies, including programs to train judiciaries on handling internet-related crimes (Saleem et al., 2025) and issuing public cybercrime warnings through network providers (Wortley & Prichard, 2023). Lastly, all four engage in international cooperation. China maintains bilateral cybercrime agreements, while South Africa ratified the Budapest Convention. Nigeria and Zimbabwe support African Union initiatives like the Malabo Convention and work with Interpol and regional bodies to combat transnational cyber threats and harmonize data protection standards.

Differences among the Countries

China and several African countries adopt markedly different approaches to cybersecurity governance. According to Cui and Qi (2021), China enforces strict data localization requirements, centralized control over cyberspace, real-time surveillance, and tight restrictions on cross-border data transfers. In contrast, many African nations, including South Africa, Nigeria, and Zimbabwe, typically rely on foreign data servers, which complicates investigations and limits national jurisdiction. While these African countries have criminalized various forms of cybercrime, enforcement is often hampered by resource limitations, insufficient technical expertise, and inadequate law enforcement capacity (Mphatheni & Maluleke, 2022). Moodley (2024) recounts a tragic South African case where law enforcement was unable to investigate an online extortion-induced suicide due to technical limitations. Additionally, whereas China exercises extensive content control and censorship, most African countries pursue a rights-based approach, seeking to balance regulation with freedom of expression, although occasional restrictions occur in some states. In terms of international engagement, China prefers bilateral cybersecurity agreements, resisting multilateral frameworks like the Budapest Convention, while African countries participate in regional or international cybersecurity initiatives, with South Africa notably ratifying the Budapest Convention.

Limitations in the implementation of cyber legislation across China, South Africa, Nigeria, and Zimbabwe.

On the other hand, critics argue that cybersecurity laws in several countries are often used to censor and restrict online speech, particularly on sensitive political topics, rather than to protect vulnerable groups effectively (Li, 2023). In China, the lack of transparency in the implementation and enforcement of these laws, combined with the government's tight control over the internet, has made it difficult for women and children to seek redress for online harms. Another concern is that Chinese cyber laws overly protect government interests and fail to clearly define what constitutes a violation. This ambiguity creates uncertainty, instills fear among citizens, and raises concerns about unwarranted government surveillance (Li, 2023). In Zimbabwe, a significant issue is the lack of a cybersecurity culture and effective national response. According to Poshai, Chilunjika, and Intauno (2023), the country has made limited progress in promoting cybersecurity awareness and combating cybercrime. Moyo, Makota, and Kabote (2024) further highlight the shortage of cybersecurity professionals, which is exacerbated by weak policy frameworks and the absence of structured implementation programs. Nigeria's cybersecurity laws have similarly come under criticism. Rather than safeguarding vulnerable groups, the laws have been used to suppress journalists and enable widespread monitoring of citizens (Bello & Griffiths, 2021). The enforcement of these laws is inadequate, and there is little accountability for companies that mishandle or sell individuals' personal data. As a result, organized cybercrime continues to flourish, leaving many Nigerians exposed (Bello & Griffiths, 2021). In South Africa, the slow implementation of cybersecurity laws has raised alarms about the country's capacity to respond to rapidly evolving cyber threats. Nte, Enoke, and Teru (2022) point out that law enforcement agencies lack both training and resources, limiting their ability to respond effectively to cybercrime.

Comparative advantages inherent in China's approach to combating cybercrime

China has effectively imposed restrictions on foreign applications that store user data on servers located outside its borders, including in countries such as the United Kingdom and the United States (Rolf & Schindler, 2023). The reliance on privately owned foreign servers poses significant challenges to ensuring data privacy and protecting the personal information and online activities of individuals. By requiring that data generated within China be stored on domestic servers governed by national legislation, the Chinese government enhances its capacity to regulate cyberspace and facilitate the prosecution of cybercrimes, thereby providing victims with greater access to justice (Zhang & Gong, 2024). For instance, instead of widely used global applications such as WhatsApp, Chinese citizens use domestically developed platforms like WeChat, which operate under national cybersecurity regulations. Additionally, regulatory authorities oversee and strictly control the export of data, minimizing the risk of unauthorized transfers. This comprehensive framework was achieved through sustained policy efforts that en-

couraged domestic innovation and fostered competition within the country's digital economy.

5. Limitations of the Study

The study had a few limitations, such as relying on secondary information, which may be unable to capture the timeliness of information, and no new research was conducted. This is because of the distance among these countries, and this may have limited the validation of findings and deeper insights from participants in the cyber law field. There is also the absence of cybercrime statistics on cybercrimes against women and children, as they were not available on the official police and other state websites, and the ones that were available had no official translation. This limited the ability to provide a quantitative basis for conclusion. The limitations highlight the need for caution in interpreting the findings and suggest opportunities for future research using primary data and statistical evidence.

6. Recommendations and Conclusions

There is a pressing need for the effective enforcement of cybersecurity laws and the establishment of specialized courts to address cybercrimes. Governments should prioritize public education, particularly for parents and young people, to raise awareness about online risks. With the rapid development of technologies such as Artificial Intelligence, it is important for governments to enforce cyber laws and strictly regulate data. They should also educate the public on Artificial Intelligence safety measures as it may be used to harm young women and children by generating images in their likeness. Cybersecurity legislation must be adaptable, continuously evolving with technological advancements. Governments should facilitate cooperation among government agencies, private and public companies, and civil society to ensure the sharing of valuable information. Additionally, robust data protection policies are essential to reinforce these laws. International cooperation remains vital, as diplomatic relations can facilitate cross-border investigations and coordinated cyber threat responses. Both China and several African countries recognize the importance of strengthening cybersecurity frameworks. In South Africa, continuous evaluation and increased investment in cybersecurity research are needed to enhance implementation. Zimbabwe should foster an environment that promotes cybersecurity research and incident reporting, enabling institutions to improve detection and response strategies. Furthermore, Zimbabwe and Nigeria would benefit from developing clear, specific, and well-defined laws to ensure consistent interpretation and effective judicial application.

In conclusion, it is important to critically examine the progress made by China in safeguarding young women and children in digital spaces, particularly through stringent data protection measures. These regulations significantly reduce the risk of personal data being sold online and facilitate more effective investigations into cyber offenses. In contrast, South Africa has introduced legal frameworks and

maintained cooperative diplomatic relations with international organizations to enhance online safety for vulnerable groups. However, Nigeria continues to face persistent challenges, with high rates of cybercrime and limited enforcement capacity due to resource constraints. Similarly, Zimbabwe lacks comprehensive documentation of cybercrime incidents and suffers from insufficient training and resources necessary for effective investigations, reflecting a broader issue within the country's cybersecurity governance. Cybersecurity in Zimbabwe is often treated as a secondary concern, leaving many citizens unaware of the risks they face online. As digital technologies expand, they increasingly serve as double-edged swords, offering opportunities for empowerment while simultaneously providing new platforms for the perpetration of violence against women and girls. Without sustained and coordinated efforts to strengthen cybersecurity frameworks in these countries, the risks posed by technological advancement to vulnerable populations will only intensify.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Ateş, E. C., Bostanci, E., & Guzel, M. S. (2018). Cybercrimes against Children in Turkey. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-6). IEEE. https://doi.org/10.1109/isdfs.2018.8355374

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and Global Regulatory Challenges. *Journal of Financial Crime, 28,* 359-374. https://doi.org/10.1108/jfc-07-2020-0149

Bello, M., & Griffiths, M. (2021). Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable Are Law Enforcement Agencies? In *Rethinking Cybercrime* (pp. 213-235). Springer. https://doi.org/10.1007/978-3-030-55841-3_11

Bofu-Matinha, M. (2024). Cybersecurity Awareness Taken to Rural Areas. *ZBC News*. https://www.zbcnews.co.zw/cyber-security-awareness-taken-to-the-rural-communities/

Bucy, E. P. (2000). Social Access to the Internet. *Harvard International Journal of Press/Politics, 5,* 50-61. https://doi.org/10.1177/1081180x00005001005

Butt, E. (2024). *Amanda Todd Case. The Canadian Encyclopaedia*. https://www.thecanadianencyclopedia.ca/en/article/amanda-todd-case

China Internet Network Information Center (CNNIC) (2024). *The 53rd Statistical Report on China's Internet Development*. http://www.cnnic.com.cn

Chingoriwo, T. (2022). Cybersecurity Challenges and Needs in the Context of Digital Development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies, 3,* 77-104. https://doi.org/10.37745/bjmas.2022.0046

Chipfumbu, C. T., Tsokota, T., & Marovah, T. (2024). Cyber-Security Awareness and Its Contribution towards Sustainable Human Development: Insights from the Zimbabwean Context. *International Cybersecurity Law Review, 5,* 347-364. https://doi.org/10.1365/s43439-024-00120-6

Chiu, H. (1985). The 1982 Chinese Constitution and the Rule of Law. *Review of Socialist Law, 11,* 143-160. https://doi.org/10.1163/187529885x00106

Cowling, N. (2024). Digital Population in South Africa as of 2020. *Statistica*. https://www.statista.com/statistics/685134/south-africa-digital-population/

Cui, S., & Qi, P. (2021). The Legal Construction of Personal Information Protection and Privacy under the Chinese Civil Code. *Computer Law & Security Review, 41,* Article 105560. https://doi.org/10.1016/j.clsr.2021.105560

Cuihong, C. (2018). China and Global Cyber Governance: Main Principles and Debates. *Asian Perspective, 42,* 647-662. https://doi.org/10.1353/apr.2018.0029

Data Reportal Global Digital Insights (2024). *Data Reportal Global Digital Insights Internet use 2024*. https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption

Deora, R. S., & Chudasama, D. (2021). Brief Study of Cybercrime on the Internet. *Journal of Communication Engineering & Systems, 11,* 1-6.

Department of Basic Education, Republic of South Africa (2024). *DBE and Google Enter Partnership to Fight Cybercrimes Targeted at School-Going Children*. https://www.education.gov.za/ArchivedDocuments/ArchivedArticles/DBE-Google-partnership-to-fight-cybercrimes-0624.aspx

Faith, B. (2022). Tackling Online Gender-Based Violence; Understanding Gender, Development, and the Power Relations of Digital Spaces. *Gender, Technology and Development, 26,* 325-340. https://doi.org/10.1080/09718524.2022.2124600

Galal, F. (2024). Internet Usage in Africa—Statistics & Facts. *Statistica*. https://www.statista.com/topics/9813/internet-usage-in-africa/#topicOverview

Government of South Africa (2021). *Cybercrimes Act 19 of 2020*. Government Gazette. https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

Greiman, V. A. (2022). Cyber Law and Regulation. In *Cyber Security: Critical Infrastructure Protection* (pp. 59-78). Springer International Publishing.

Harkin, D., & Whelan, C. (2022). Perceptions of Police Training Needs in Cyber-Crime. *International Journal of Police Science & Management, 24,* 66-76. https://doi.org/10.1177/14613557211036565

Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *Journal of Cybersecurity and Privacy, 1,* 580-596. https://doi.org/10.3390/jcp1040029

Ibekwe, C. R. (2015). *The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions*. University of Stirling.

Jane, E. A. (2020). *Online Abuse and Harassment. The International Encyclopedia of Gender, Media, and Communication*. https://www.onlinelibrary.wiley.com/doi/10.1002/9781119429128.iegmc080

Kahn, R. E., & Cerf, V. G. (1999). II. What Is the Internet (and What Makes It Work)? *Open Architecture, 17,* 2.

Kamble, R. M. (2013). Cyber Law and Information Technology. *International Journal of Scientific & Engineering Research, 4,* Article 789.

Kemp, S. (2024a). Digital 2024: Nigeria. *Datareportal*. https://datareportal.com/reports/digital-2024-nigeria

Kemp, S. (2024b). Digital 2024: Zimbabwe. *Datareportal*. https://datareportal.com/reports/digital-2024-zimbabwe

Li, G. (2023). Internet Censorship in China: A Functioning Digital Panopticon. In *Communications in Contemporary China* (pp. 11-26). Routledge.

Lindsey, L. L. (2020). *Gender: Sociological Perspectives*. Routledge.

Liu, L. (2021). The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development, 56,* 45-67. https://doi.org/10.1007/s12116-021-09319-8

Lu, F. (2023). 'Pink Hair Prostitute' Taunts Drive Woman, 23, to Suicide Following 6 Months of Online Abuse; Millions in China Mourn Death. *South China Morning Post.* https://www.com/news/people-culture/trending-china/article/3210853/bullied-death-millions-chinese-mourn-after-prostitute-pink-hair-taunts-drive-woman-23-suicide

Ma, R. (2024). The Comparison and Conflicts of the Cross-Border Criminal Data Retrieval between Europe and China. *The Modern Language Journal, 5,* Article 42.

Madhuku, L. (2010). *An Introduction to Zimbabwean Law.* African Books Collective.

Masiphephe Network (2023). *The Impact of Cyberbullying in South Africa. USAID and Center for Community Impact.* https://www.masiphephe.org.za/wp-content/uploads/2023/05/3.-Thematic-paper-cyber-bullying-in-SA_FINAL.pdf

Matsaung, L., & Masiloane, D. (2024). Cyber-Intelligence Practices of South African Police Officials in the Investigation of Cybercrime: Some Conceptual Issues. *African Security Review, 33,* 178-198. https://doi.org/10.1080/10246029.2024.2421225

Modise, J. M. (2025). The Impact of Capacity Building Initiatives on the SAPS's Ability to Investigate and Prosecute Cybercrime. *IRASS Journal of Arts, Humanities and Social Sciences, 2,* 78-85.

Mokofe, W. M. (2023). Digital Transformations of the South African Legal Landscape. *Journal of Digital Technologies and Law, 1,* 1087-1104. https://doi.org/10.21202/jdtl.2023.47

Moodley, N. (2024). Online Threat: Sextortion—Frantic Teens Trapped by Blackmailers on Social Media. *Daily Maverick.* https://www.dailymaverick.co.za/article/2024-08-18-sextortion-frantic-teens-trapped-by-blackmailers-on-social-media/

Moyo, A., Makota, J., & Kabote, F. (2024). Changes in the Data and Information Systems in Zimbabwe: Lessons from Legislation and Policy Post 2018. *Lighthouse: The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy, 3,* 1-15. https://doi.org/10.71458/fzkj8n13

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a Response to Combating Cybercrime: Demystifying the Prevailing Threats and Offering Recommendations to the African Regions. *International Journal of Research in Business and Social Science, 11,* 384-396.

Mugari, I. (2020). The Dark Side of Social Media in Zimbabwe: Unpacking the Legal Framework Conundrum. *Cogent Social Sciences, 6,* 1-15. https://doi.org/10.1080/23311886.2020.1825058

Mugari, I., Kunambura, M., Obioha, E. E., & Gopo, N. R. (2023). Trends, Impacts and Responses to Cybercrime in the Zimbabwean Retail Sector. *Safer Communities, 22,* 254-265. https://doi.org/10.1108/sc-03-2023-0011

National People's Congress of China (2016). *Cybersecurity Law of the People's Republic of China.* http://www.cac.gov.cn/

Nayak, S. K., & Bello, A. (2024). Evaluating the Effectiveness and Gaps in Nigeria's Government Cybersecurity Policies: Recommendations for Enhancing Cybersecurity Measures. *Journal of Systematic and Modern Science Research, 5,* 1-22.

Ngcece, S., Mkhize, S., & Majola, K. B. (2025). Exploring Responses to Cybercrime in South Africa: The South African Police Services (SAPS) Perspectives. Journal of Cyberspace

Studies, (), 1-21. https://doi.org/10.22059/jcss.2025.395262.1149

Nigeria Cybercrimes Act (2015). *Cybercrimes (Prohibition, Prevention, etc.) Act 2015*. Federal Government of Nigeria. https://www.nitda.gov.ng

Nte, N. D., Enoke, B. K., & Teru, V. A. (2022). A Comparative Analysis of Cyber Security Laws and Policies in Nigeria and South Africa. *Law Research Review Quarterly, 8,* 233-258. https://doi.org/10.15294/lrrq.v8i2.56486

Nwosu, E. (2015). *Nigeria. Millennium Goals and NEEDS: The*.

Obidimma, E. O. C., & Ishiguzo, O. (2023). Cybercrime Investigation and Prosecution in Nigeria: The Critical Challenges. *African Journal of Criminal Law and Jurisprudence, 8,* Article 30.

Parliament of Zimbabwe (2021). *Cybersecurity and Data Protection Act*. Government of Zimbabwe. https://www.ictministry.gov.zw/wp-content/uploads/2024/01/Cyber-and-Data-Protection-Act-Chapter-1207.pdf

Plan International (2022). *Design Thinking Helps Children Explore Online Safety*. https://plan-international.org/china-en/case-studies/design-thinking-helps-children-explore-online-safety

Poshai, L., Chilunjika, A., & Intauno, K. (2023). Examining the Institutional and Legislative Frameworks for Enforcing Cybersecurity in Zimbabwe. *International Cybersecurity Law Review, 4,* 431-449. https://doi.org/10.1365/s43439-023-00093-y

Powell, C., & Schonwetter, T. (2019). Africa, the Internet and Human Rights. In *Human Rights, Digital Society and the Law* (pp. 319-336). Routledge. https://doi.org/10.4324/9781351025386-22

Proulx, K. (2022). *Anonymity Online and the Perfect Environment for Cybercrime*. Master's Thesis, Utica University.

Pyo, G. (2021). An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts. *Columbia Journal of Transnational Law, 60,* Article 228.

Rolf, S., & Schindler, S. (2023). The US-China Rivalry and the Emergence of State Platform Capitalism. *Environment and Planning A: Economy and Space, 55,* 1255-1280. https://doi.org/10.1177/0308518x221146545

Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). Challenges Faced by the Judiciary in Implementing Cybersecurity Laws in Pakistan. *The Critical Review of Social Sciences Studies, 3,* 1052-1066. https://doi.org/10.59075/1wyx0v30

Savaş, S., & Karataş, S. (2022). Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance. *International Cybersecurity Law Review, 3,* 7-34. https://doi.org/10.1365/s43439-021-00045-4

Shackelford, S. (2016). Human Rights and Cybersecurity Due Diligence: A Comparative Study. *University of Michigan Journal of Law Reform, 50,* Article 859. https://doi.org/10.36646/mjlr.50.4.human

Sharma, R. (2023). Importance of Cyber Security. *Indian Journal of Law and Legal Research, Vol. V,* 8.

Shekhawat, H. (2022). Cyber Crimes Against Women. *International Journal of Law Management & Humanities, 5,* Article 1673.

Smit, S. T. (2024). *A Look at Victim Experiences of Cybercrime in South Africa and Whether the Current Legislative Framework Is Equipped to Deal with This Issue*. Thesis, University of Cape Town.

Snail ka Mtuze, S., & Musoni, M. (2023). An Overview of Cybercrime Law in South Africa.

International Cybersecurity Law Review, 4, 299-323. https://doi.org/10.1365/s43439-023-00089-8

South African Government (2023). *Film and Publication Board Welcomes Sentencing of Gerhard Ackerman on Charges of Possession of Child Pornography*. Republic of South Africa. https://www.gov.za/news/media-statements/film-and-publication-board-welcomes-sentencing-gerhard-ackerman-charges

South African Police Service (2015). *Child Pornography Investigation Ready for Trial: Court Told*. https://www.saps.gov.za/newsroom/msspeechdetail.php?nid=5067

South China Morning Post (2023). China Sets New Cyber Safety Rules to Protect Minors. *Young Post*. https://www.scmp.com/yp/learn/learning-resources/english-exercises/article/3242332/study-buddy-challenger-china-sets-new-cyber-safety-rules-protect-minors

Stoilova, M., Livingstone, S., & Khazbak, R. (2021). I*nvestigating Risks and Opportunities for Children in a Digital World: A Rapid Review of the Evidence on Children's Internet Use and Outcomes*.

The Herald (2024). ZRP Hosts Africa Surge Operation Meeting. *The Herald*. https://www.herald.co.zw/zrp-hosts-africa-surge-operation-meeting/

Tomlinson, K. D. (2016). An Examination of Deterrence Theory: Where Do We Stand. *Probation Journal, 80,* s33.

Unit, I. C. T. Cybercrime, & Cyber Law in Nigeria (2023). *An Overview of Challenges and Way Forward*. https://www.researchgate.net/publication/381958089_Cybercrime_and_Cyber_Law_in_Nigeria_An_Overview_of_Challenges_and_Way_Forward

United Nations General Assembly (1989). *Convention on the Rights of the Child*. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

van Niekerk, G. J. (1998). A Common Law for Southern Africa: Roman Law or Indigenous African Law. *Comparative and International Law Journal of Southern Africa, 31,* 158-173.

Vanguard.com (2017). Breaking: Killers of Cynthia Osokogu Sentenced to Death. *Vanguard*. https://www.vanguardngr.com/2017/03/breaking-killers-cynthia-osokogu-sentenced-death/

Wang, S. Y. K., Hsieh, M. L., Chang, C. K. M., Jiang, P. S., & Dallier, D. J. (2021). *International Journal of Offender Therapy and Comparative Criminology, 65,* 390-408. https://doi.org/10.1177/0306624x20952391

Wortley, R., & Prichard, J. (2023). Online Messaging as a Cybercrime Prevention Tool in the Post-Pandemic Age. In *Cybercrime in the Pandemic Digital Age and beyond* (pp. 209-232). Springer International Publishing.

Xinhua (2024). *China's Internet Users Reach 1.09 bln*. The State Council, The People's Republic of China. https://english.www.gov.cn/archive/statistics/202403/22/content_WS65fd41dac6d0868f4e8e5583.html

Zhang, H., & Gong, X. (2024). The Research on an Electronic Evidence Forensic System for Cross-Border Cybercrime. *The International Journal of Evidence & Proof, 28,* 21-44.

Appendix: Summary Table

Country	Key Offenses in Law	Typical Penalties	Enforcement Capacity
China	Cyber-pornography, child exploitation, cyber-bullying, online harassment	Strict prison terms and heavy fines of up to 1 million yuan.	Centralized enforcement agencies, advanced surveillance, but strong state control focus.
South Africa	Cyber harassment, revenge pornography, cyber-stalking, child pornography	Prison sentence of up to 15 years and Rand 50 000 in fines	SAPS cybercrime unit established, but with limited skills and resources.
Nigeria	Cyber-stalking, child exploitation, online fraud, pornography	3 years and more includes fines of more than 20,000,000 Naira, harsher for child exploitation.	Cybercrime Act enforced by EFCC and police, but with limited technical capacity.
Zimbabwe	Child pornography, online harassment, harmful digital communications	Prison sentences of up to 15 years and fines	New Cyber and Data Protection Act (2021), limited enforcement structures, resource constraints