International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cybercrime: A Comparative Analysis of Cyber Laws In Uganda and Indonesia, Examining the Effectiveness of the Enacted Legislation

Namukose Lilian[1], Muchamad Iksan[2]

[1]Student, Department of law, Universitas Muhammadiyah Surakarta
[2]Professor, Department of law, Universitas Muhammadiyah Surakarta

Abstract
The unsolicited nature of the Internet in which anybody publishes anything at any time lands a serious security threat to any nation and this goes down to personal social behavior of an individual creating both negative and positive effects, this result into multiple functionalities and freedom of use while in the cyberspace and this brings an equal ease of committing immoral acts and crimes. This research will use a comparative approach, analyzing legal principles, systematics and relevant facts, with key legislations for instance, in 2024, Uganda experienced a sharp surge in cybercrimes, leading to significant financial losses, however, the police enhanced their digital forensic capabilities to keep up with cybercrime trends and improve their ability to gather evidence thus the establishment of the computer misuse Act. More like Uganda, Indonesia also faces the same problem and is increasingly susceptible to cyberattacks, manifesting in forms such as financial fraud, cyber espionage, and ransom-related extortions due to the rapid digitalization outpacing security, a large and vulnerable internet user base with low digital awareness, weaknesses in law enforcement's technical capabilities, and a less developed cybersecurity regulatory framework.

Keywords: cyber-crime; policy making; economic loss; Uganda; Indonesia.

1. Introduction

Uganda, a small landlocked nation in East Africa, has an estimated population of about 48 million people, with roughly 26-27% residing in urban areas. As of 2024, Data Reportal Global Digital Insights estimated that 13.3 million Ugandans were using the internet. Cyberspace represents the virtue environment created by internet use; however, low levels of cyber risk awareness and limited resources leave many Ugandans vulnerable to online threats. In January 2024, the country's internet penetration stood at 27% of the total population equivalent to 13.3 million users. This marked an increase of 1.2 million users, or 10.3% compared to the period between January 2023 and January 2024[1]. The Uganda communications commission (UCC) also reports a substantial increase in internet subscriptions, showing a consistent trend of growing connectivity. However, there's a challenge of cyber threats like fishing, fraud, scamming which in simple terms is known as cyber-crimes.

[1]Kemp, Simon**.** *Digital 2024: Uganda* — Global Digital Insights (DataReportal). 23 February 2024. Available at Dataportal: "Digital 2024: Uganda".

Cybercrime is any activity that involves a computer, network, or networked device. It's a crime in the digital age, ranging from hacking and spreading viruses to online fraud, digital theft and child pornography.

The United Nations has pointed out that cybercrime covers a wide range of offences, which generally fall into two categories: cyber-enabled and cyber-dependent crimes. Cyber-enabled crimes are traditional offences that have moved online, like trafficking, fraud, or spreading hate and violence. Cyber-dependent crimes, by contrast, exist only because of technology things like phishing, identity theft, or attacks using malware and ransomware. The people behind these crimes can be lone individuals or organized groups, all taking advantage of how easy and anonymous the digital world can be.

The scope of cybercrime is extensive, covering everything from network breaches to personal exploitation. These offenses include, but are not limited to; hacking and distributing viruses, acts of cyber terrorism, complex financial and corporate crimes such as internet fraud, industrial espionage and intellectual property infringement; personal violations like impersonation and digitally facilitated sexual assault or online child exploitation and illegal activities like software piracy, illegal purchase of goods and internal internet usage policy abuses.

Acknowledging that regulations governing internet usage protect victims of cyber crime by working as a deterrent and a means of possible compensation of victims[2], Ugandan law specifically addresses these concerns through a well develops legal framework. This regulation is primarily anchored in the Computer Misuse Act, 2011, which expressly defines and regulates computer crime by establishing core offenses such as Unauthorised Access and Access with Intent to Commit or Facilitate a further offence, among other related computer- specific violations. This framework was then significantly strengthened by the computer Misuse (Amendment), Act 2022, which broadened the scope of protection and criminal liability by introducing new provisions specifically targeting modern online harms, including the sharing of unsolicited, malicious, or false information, the unauthorised sharing of information about children, and the distribution of hate speech online.

In this paper, I adopt the term crime as defined under the Computer Misuse Act, 2011, as amended in 2022. I recognise that the existing legal framework governing cyberspace in Uganda offers victims of cybercrime a certain degree of protection, both by deterring offenders and by creating avenues for possible compensation. My interest is in understanding who commits these internet-based offences, the challenges victims encounter when attempting to report them, and the measures policymakers in Uganda have implemented to curb the misuse of digital technologies.

To achieve this, I gathered information directly from internet users across Uganda and analysed the data using SPSS. My study seeks to identify where incidents are typically reported and how different individuals perceive or participate in a cybercrime related role. I employed a mixed methods approach that included a web-based survey, telephone interviews, email statements, questionnaires, and case studies. These tools enabled me to capture a comprehensive view of both the experiences of users and the broader context of cybercrime in Uganda.

Discussions and results;

2. Cybercrime in Uganda;

According to parliament watch Uganda, the official online newsletter for the parliament of Uganda, a sha-

[2] Section 27 of the computer misuse Act.

dow minister for ICT honourable Hellen Nakimuli called for an increased investment in Uganda's cyber security following a high-risk strike rate in cyber crime which surged by 93.5% in 2024 resulting to a high rate of financial loss amounting to UGX 2.125 billion of which only ugx 420 million was recovered[3].

The low digital literacy rates among Ugandans have also proves to be one of the reasons for the increased cybercrime in most of the areas as cyber criminals are finding more opportunities to exploit people's vulnerability and ignorance, local media approves that large segments of the population remain offline regardless of the broadband availability, and identifies digital illiteracy as a central challenge[4].

In Uganda, a severe lack of digital skills is a major impediment to mobile internet use, even for those who are aware of its benefits, preventing many from performing basic functions like digital payments. This deficiency highlights by a 33% score on digital skill in the 2021 inclusive digital economy scorecard creates a population highly susceptible to safety and security risks[5]. The country is currently battling a rise in cyber dependent crimes, primarily unauthorised system access, malware distribution, and the exploitation of evolving remote work setups. Furthermore, insider threats frequently target startup companies. A significant challenge remains in addressing these crimes, as many go unreported, and law enforcement agencies often do not investigate them or assess their financial impact, as documented by the Global Organised Crime index.

Table1; showing performance data cybercrime department from 2019-2024

YEAR	OPENING STOCK	RECEIVED	ALL CASES (OPENING STOCK + RECEIVED	PROCESSED	% (PROCESSED OF ALL OUTSTANDING CASES)	BACKLOG
2019	140	226	366	124	34%	242
2020	242	260	502	180	36%	322
2021	322	330	652	167	26%	485
2022	485	414	899	382	42%	517
2023	517	586	1103	523	47%	580
2024	580	738	1318	446	34%	872

As illustrated in Table 1, the total number of reported cases rose consistently from 366 in 2019 to 1,318 in 2024. This upward trend indicates that the department has faced an expanding caseload, likely driven by a heightened need for its services. The cases handled ranged from bank fraud, unauthorized access to digital systems, and intrusions into banking platforms, to investigations involving fraudulent practices

[3] Parliament Watch. "Opposition Raises Alarm Over Uganda's Surging Cyberattacks." 25 March 2025.
[4] Business Times Uganda. "Uganda's Digital Leap: Fast Connections, Slow Adoption – GSMA Report." *Business Times Uganda*, 2025.
[5] UNCDF. "Government of Uganda Releases Inclusive Digital Economy Scorecard (IDES) 2021 report." 23 September 2021.

within the Uganda Wildlife Authority aimed at preventing government revenue losses in national parks, as well as matters related to corruption, cyber harassment, and other offences[6].

Despite the rising number of cases, the rate of case processing has shown considerable variations; 34% in 2019, 36% in 2020, 26% in 2021, 42% in 2022, 47% in 2023 and 34% again in 2024. According to a report by the Uganda Police Force 's Directorate of Forensic Services, the inconsistency stems from the increasing sophistication of the cases and persistent limitations in resources, including staffing and technological capacity[7].

Research indicates that many internet users in Uganda are simultaneously victims and perpetrators of cybercrime, with most victims failing to report incidents to the police. The majority of cases have cross-border dimensions, involving actors from countries such as Nigeria, Congo, Kenya, and Canada, who exploit Uganda's low-skilled internet users. Despite these challenges, Uganda has signalled its intention to join international frameworks, including the Council of Europe Convention, and has sought to align its national legislation particularly the Computer Misuse Act with global standards, though these efforts have yet to succeed.

3. Cybercrime in Indonesia;

Cyberattacks targeting Indonesia have had a significant impact on both the public and private sectors. Some of the largest cyberattacks in Indonesia have not only damaged the reputation of many institutions but has also caused significant financial losses. Indonesia has been identified as the country with the highest ransomware threat in the ASEAN region. Credible reporting from CIO World Asia, The Jakarta Post, and detikcom indicates that in August 2024, Indonesia experienced a major cybersecurity breach involving approximately 4.7 million records of civil servants (PNS/ASN) managed by BKN, with the stolen data later posted on a dark-web marketplace[8]. Several local and international outlets, including The Star and detikfinance, also confirmed that a hacker using the alias "TopiAx" claimed responsibility for stealing and attempting to sell the data.[9] The leaked information reportedly contained sensitive personal details such as names, NIP (civil-servant ID numbers), dates of birth, and employment information as further highlighted by detikcom and Harianjogja.com. In addition to this 2024 breach, earlier cybersecurity assessments, including analyses published through Econstor and E-Journal UMM, note that the National Cyber and Crypto Agency (BSSN) recorded approximately 290 million cyber-attack attempts in 2019, reflecting the scale and persistent nature of Indonesia's cybersecurity challenges.[10]

The heightened threat of cyberattacks such as phishing, malspam, and ransomware that merged during the 2020 COVID-19 pandemic emphasizes the need for a functional cybersecurity infrastructure in Indonesia. In response, a cohesive criminal system has been established, integrating the police, prosecutors, courts and correctional facilities. The combined effort of these four components is formalised through legislation like the Electronic Information and Transaction (ITE) Law and the personal data protection (PDP) Law,

[6] Uganda Police Force. "Digital Forensics Services Annual Performance Report 2024." Kampala: Uganda Police Force, Directorate of Forensic Services, 2025.

[7] Uganda Police Force, Directorate of Forensic Services. Annual Forensic Services Performance Report. Kampala: Uganda Police Force, 2024.

[8] CIO World Asia Newsroom, "Cyberattack Exposes Over 4.7 million Records – Indonesia's National Civil Service Agency Breached," August 15, 2024 and The Jakarta Post, "Fresh data breach puts pressure on government to form cyber privacy agency," August 13, 2024.

[9] detikFinance. "Geger Data 4,7 Juta ASN Bocor dan Dijual Rp 159 Juta." August 12, 2024. Accessed https://finance.detik.com/berita-ekonomi-bisnis/d-7484912/geger-data-4-7-juta-asn-bocor-dan-dijual-rp-159-juta.

[10] ItWorks (citing BSSN): "Pusopkamsinas BSSN Mencatat 290,3 Juta Serangan Siber Menyasar Indonesia".

both of which criminalise digital crimes. The Indonesian government has also integrated the cybercrime law (UU cyber) into ITE Law (most recently amended by Law No. 19 of 1026).

The legal foundation is intended to be the primary tool for combating, reducing and preventing crimes in the digital space. Specific supplementary regulations proposed by Hardin Anto, Al QADRI, and Faudy (2021) are scheduled to be analysed in the following sections below;

- Article 2 of the ITE law 2008, presents the provisions concerning online gambling.
- Article 27 of the ITE law 2008, presents the provisions concerning defamation and threats which are made in a cyberspace.
- Article 28 of the ITE law 2008, presents the provisions concerning false accusations and news which are spread online.
- Article 29 of the ITE law 2008, presents the provision concerning violence which takes place in an online medium.

Despite Indonesia's increasing dependence on digital technologies, its legal system does not yet have a single comprehensive statute dedicated specifically to cyber law, creating a need for greater clarity and transparency in regulating cyberspace. To address this gap, the government has enacted several laws aimed at preventing and responding to cyber-related offences, including Law No. 36 of 1999 on Telecommunications, Law No. 19 of 2002 on Copyright, and Law No. 19 of 2016 on Information and Electronic Transactions (ITE Law). The ITE Law itself contains two broad categories of provisions those governing information and electronic transactions and those prohibiting various forms of cybercrime and many of its cybercrime-related articles draw conceptual influence from the EU Convention on Cybercrime, a widely used international framework, even though Indonesia has not formally become a signatory.

However, international bodies like the United Nations and the Council of Europe emphasize that cybercrime is a transnational issue requiring international cooperation and integration with international standards, such as the Budapest Convention, for Indonesia to effectively combat cross-border attacks and strengthen its cybersecurity framework. This measure will encourage individuals to report serious cybercrime incidents. It is expected that such an approach will contribute to reducing the occurrence of cybercrimes not only in Indonesia but also in other countries.

4. Specific cases;

1) On February 6, 2025, eight officials from Uganda's Ministry of Finance were officially brought before the court to face charges of corruption, electronic fraud, and money laundering. These charges stemmed from a hacking incident in 2024 that targeted the central bank's systems, resulting in the theft of at least $21 million. Court documents indicate the scheme involved diverting intended payments to unauthorized recipients. Crucially, the fraud was initiated *outside* the Bank of Uganda's IT systems, exploiting its role as a paying entity to reroute the funds[11].

2) This incident, which confirms local media reports from last November, illustrates a major breach involving the central bank's accounts where funds were illegally diverted, as confirmed by State Minister for Finance Henry Musasizi. Specifically, funds intended for loan principal and interest repayments to the

[11] Lubowa, Abubaker. "Uganda charges finance ministry officials with corruption, money laundering." *Reuters*, February 7, 2025. https://www.reuters.com/world/africa/uganda-charges-finance-ministry-officials-with-corruption-money-laundering-2025-02-07/

World Bank's International Development Association (IDA) were redirected to companies in Japan and Poland. According to the charge sheet, one ministry official, an IT officer, "irregularly altered the payment instructions" to divert IDA funds to a Tokyo-based company, with another portion also being illegally paid out to a company in London. Consequently, several high-ranking ministry officials, including the top accountant, now face serious charges including corruption, causing financial loss, electronic fraud, money laundering, and abuse of office for their roles in this theft.[12] The first heist was the spiriting away of $6.134m (22.3b) which happened in early September 2024, but Uganda's ministry of finance by omission or commission, kept lead on the matter until IDA flagged the late payment in early October. Even then, according to sources, it took another month for the ministry to call in the Auditor General's office. The heist according to the information systems audit codenamed "project Tai" undertaken by PricewaterhouseCoopers (PwC), involved computer experts and accountants manipulating financial information inside the government's digital cash transaction portal, the integrated facility management system (IFMS), with the stroke of a few keys on the computer.

3) A recent BBC investigation exposed a Ugandan businessman based in Dubai, Abbey Mwesigwa, who reportedly lures young women from Uganda and other African countries with promises of legitimate employment such as supermarket attendants or nannies. However, these women are then allegedly sold into prostitution. According to the report, "Young Ugandan women told us they had not expected to have to undertake sex work for Mr. Mwesigwa. In some cases, they believed they were travelling to the UAE to work in places like supermarkets or hotels." One interviewee, "Mia," stated that one of Mr. Mwesigwa's clients regularly engaged in extreme sexual acts, and she felt trapped by his network. Mwesigwa is said to use an online platform known as "Dubai portapotty," associated with the hashtag #Dubaiportapotty, which has garnered over 450 million views on TikTok. This hashtag often features parodies and speculative content about women supposedly funding luxurious lifestyles through extreme sexual requests. Shockingly, Mwesigwa admitted to having access to Uganda's National Identification and Registration Authority System, which issues national ID cards, and also claimed connections with officials in the Ministry of Internal Affairs responsible for issuing passports.[13]

4) By mid-2025, the Indonesia Anti-Scam Centre (IASC) under OJK had recorded over 157,000 fraud-related complaints, with estimated losses reaching approximately Rp 3.2 trillion (about US$200 million). The most frequently reported schemes involved online shopping fraud, phishing attempts, investment scams, and impersonation of officials or banking staff. From its launch in November 2024 through mid-2025, the centre received a steadily increasing volume of reports rising from around 79,969 cases in March 2025 to more than 128,000 by late May. Across this period, OJK and its partner agencies assessed that the total financial losses likely fell between Rp 2.1 trillion and Rp 3.2 trillion, depending on the estimates and exchange-rate calculations. These figures are drawn from IASC/OJK monitoring updates as well as national media coverage summarizing the agency's public statements.[14]

5. Policy making and its effect;

Similar to Indonesia, Uganda possesses a strong legislative framework designed to combat transnational organised crime, largely a response to its extensive history of online activities like scams, phishing and

[12] Monitor (Uganda). "Police arrest nine govt officials over Bank of Uganda heist." February 2025. https://www.monitor.co.ug/uganda/news/national/police-arrest-nine-govt-officials-over-bank-of-uganda-heist--4913192.
[13] BBC World Service. "Boss of degrading sex-trade ring in Dubai's glamour districts unmasked by BBC." 15 September 2025.
[14] ANTARA News. "IASC OJK Ungkap Total Kerugian Korban Penipuan Online Rp 3,2 Triliun." *ANTARA News*, 26 June 2025.

money fraud. Despite having laws in place to address these persistent cybercrimes, implementation remains inadequate in both countries. Prior to 2011, Uganda lacked specific legislation to address cybercrime, meaning traditional penal statutes often failed to prosecute offenses like hacking and cyber theft, mainly due to underreporting by victims. Additionally, prosecuting cases involving forbidden system access presented significant challenges. To remedy this and ensure such online offenses could be criminalised and penalised, The Computer Misuse Act of 2011 was introduced, which has yielded some positive results, though limited.

In response to the growing threat of cybercrime, Indonesia has enacted legislation that parallels measures taken in Uganda. Notably, Indonesian lawmakers introduced Law No. 19 of 2016 on Electronic Information and Transactions (ITE), which specifically targets the spread of misinformation through digital platforms. Article 28(1) of the law prohibits the dissemination of false or misleading information in electronic transactions. This reflects a shared regulatory approach in both Uganda and Indonesia aimed at reducing cyber risks, as elaborated further in this discussion. The relevant laws include:

1. Electronic fraud;

Any person who carries out electronic fraud commits an offence and is liable, on conviction, to a fine not exceeding three hundred sixty currency points or to imprisonment for a term not exceeding fifteen years, or both. (2) for the purposes of this section, "election fraud" means deception deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both[15]. In Indonesia, electronic fraud is addressed by Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) (and its subsequent amendments, particularly Law No. 19 of 2016) under Article 28 Paragraph (1), which penalizes the intentional and unauthorized spreading of false or misleading information causing consumer loss in electronic transactions. Violators can face a maximum sentence of 6 years in prison and/or a fine of up to Rp 1 billion.

2. Unauthorised access[16];

"A person who, without authorization

- accesses or intercepts any program or another person's data or information;
- voice records or video records another person; or (c) shares any information about or that relates to another person, commits an offence".

3. "Any person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data or performs any of those acts with regard to a password, access code or any other similar kind of data, commits an offence.[17] "The House of Lords, in R v Bow Street Magistrate; ex parte US Government Allison, 16 has given guidance on the liability of the perpetrator for ultra vires acts relating to computer network and system access. The court held that unauthorized access is established in the following scenarios: intentional access to specific data; access was unauthorized by a person entitled to authorize access to that computer or network; possession of knowledge by the perpetrator that the said access to the computer system was unauthorized."

Regarding the legal framework in Indonesia, my understanding is that unauthorized access to electronic

[15] Section 19 of the computer misuse act, 2011.
[16] Section 12 of the computer misuse act, 2011.
[17] Section 12(3) of the computer misuse act, 2011.

systems and data is explicitly forbidden under two major acts: the Electronic Information and Transactions (ITE) Law (Law No. 11 of 2008, as amended) and the Personal Data Protection (PDP) Law (Law No. 27 of 2022). The ITE Law strictly prohibits unauthorized interception and access[18], imposing severe penalties, including up to 10 years imprisonment and fines. Complementing this, the PDP Law focuses specifically on protecting personal data from unauthorized access, processing, and misuse. Ultimately, those who are guilty of cybercrimes acts face a maximum imprisonment of 10 years and/or a fine of up to IDR 800,000,000.

4. Unauthorized use or interception of computer service[19] (1) subject to subsection (2), a person who knowingly;

1. Secures access to any computer without authority for the purpose of obtaining, directly or indirectly, any computer services.
2. Intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device, whether similar or not; or
3. Uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (i) or (ii) commits an offence and is liable, on conviction, to a fine not exceeding two hundred forty currency points or to imprisonment for a term not exceeding ten years, or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred sixty currency points or to imprisonment for a term not exceeding fifteen years, or both. Indonesia likewise under Article 31 of the ITE law criminalizes intentionally and unlawfully intercepting electronic information or documents from another person computer or system, with penalties including up to 10 years in prison and / or a fine of up to IDR 800 million as stipulated under article 47 of the same act.

5. Unauthorized sharing of information about children[20];

A person shall not send, share or transmit any information about or that relates to a child through a computer unless;

- The person obtains the consent of the parent or guardian of the child, or other person having authority to make decisions on behalf of the child;
- The person is authorized by law; or
- The sending, sharing or transmitting of the information is in the best interest of the child.

Any person who contravenes section 23 of the misuse act commits an offence and is liable, on conviction, to a fine not exceeding seven hundred fifty currency points or to imprisonment for a term not exceeding seven years, or both. The laws have continually empowered authorities to prosecute and punish individuals who unlawfully share children's data without their parents' consent, particularly if it violates their privacy or well-being, with a particular focus on the "best interests of the child.

In Indonesia, the protection of children's data is governed under Law Number 27 of 2022 on Personal Data Protection (UU PDP), which establishes a comprehensive legal framework for safeguarding personal information. Article 4(2) of the PDP Law designates children's data as a category of specific personal data information that, if misused or improperly processed, could result in more severe consequences for the data subject, including discrimination or significant harm. This classification covers a wide range of information

[18] Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE), Articles 30–31.
[19] Section 15 of the computer misuse act, 2011.
[20] Section 23 of the computer misuse act, 2011.

related to children, such as their identity, location, photographs, recordings, and any other details about them, as well as their thoughts or expressions conveyed through words, audio, or images.

Furthermore, parents are urged to safeguard their children under Indonesia's Child Protection Law, specifically Law No. 35 of 2014. Article 20 of this law stipulates that "parents have the duty and responsibility to carry out child safety measures." On the international level, personal data protection is enshrined in the Universal Declaration of Human Rights (UDHR). Article 12 of the UDHR affirms that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation."

6. Cyber harassment;

Any person who commits cyber harassment is liable, on conviction, to a fine not exceeding seventy-two currency points or to imprisonment for a term not exceeding three years, or both.[21] In Indonesia, cyber harassment is primarily governed by the Electronic Information and Transactions (ITE) Law, specifically Law Number 19 of 2016 which amended the original ITE Law. The most relevant provisions are Article 27 paragraphs (3) and (4), which address defamation and stalking respectively, and the corresponding penalties outlined in Article 45 paragraph (3) and (4). These articles define prohibited actions like distributing electronic data that contains defamation or constitutes stalking and detail the potential imprisonment and fines for violation.

Section 26(4) of the electronic transaction act, A person who sends an unsolicited commercial communication to a person who has advised the sender that he or she should not send the communication, commits an offence and is liable on conviction, to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

7. Misuse of social media[22];

"A person who uses social media to publish, distribute or share information prohibited under the laws of Uganda under a disguised or false identity, commits an offence."

" Where a person is convicted under this Act, the court shall in addition to the punishment provided therein, order such person to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the aggrieved party; and such order shall be a decree under the provisions of the Civil Procedure Act, and shall be executed in the manner provided under that Act."

Indonesia's Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), along with its 2016 and 2024 amendments, serves as the foundation of the nation's digital regulatory framework by criminalizing harmful online activities. The law forbids the circulation of electronic information that contravenes societal norms, such as defamation under Article 27(3) and hate speech under Article 28(2). In addition, Article 27(2) specifies that anyone who knowingly and without authorization distributes, transmits, or provides access to electronic information or records containing gambling material is committing a criminal offence. Overall, these provisions are designed to curb online hate speech and prevent the spread of content intended to provoke hostility or conflict between individuals or groups.

[21] Section 24 of the computer misuse act, 2011.
[22] Section 29 of the computer misuse act, 2011.

Challenges;

Uganda's judicial system continues to struggle with several systemic weaknesses, including limited independence, insufficient personnel, and persistent corruption. These challenges, combined with the inherent complexities of cyber-crime enforcement experienced worldwide, hinder effective prosecution in Uganda. A major obstacle lies in the nature, quality, and admissibility of evidence presented during cybercrime trials. Evidence refers to any material capable of proving or disproving a fact in issue and may include oral testimony, documents, or physical objects, provided they meet admissibility standards. As defined in the Oxford Dictionary of Law (2002), the law of evidence encompasses the rules that regulate how facts and proof are presented before a court, including both admissibility criteria and exclusionary principles. Although evidence may be direct, circumstantial, primary, secondary, or otherwise, cybercrime cases demand a specialized approach. In this context, evidence often falls within the domain of forensic science, which applies scientific techniques to resolve questions that arise in criminal investigations and legal proceedings.

In criminal proceedings, it is a fundamental rule that the prosecution must demonstrate the accused's guilt to the high standard of beyond reasonable doubt before a conviction can be obtained. Consequently, the quality of factual and documentary evidence presented in cybercrime prosecutions is fundamental to the trial's outcome. Unfortunately, the evidence available to prosecutors is often weak, leading to many attempts to apprehend and prosecute cybercriminals being unsuccessful. Compounding this challenge is the tendency of cybercriminals to deliberately destroy evidence to evade justice. When critical digital evidence for solving a cybercrime is eliminated, investigators are frequently left with insufficient leads to pursue arrests and prosecutions.

Impersonation or identity theft is a critical tactic employed by cybercriminals that significantly complicates digital evidence. This practice is intentionally executed to misdirect and derail investigations concerning the true identity of the offender. As a result, individuals who are not responsible for the offence often find themselves arrested and charged. The nature of digital technologies enables significant identity concealment, making it extremely challenging and sometimes nearly impossible to reliably identify the true perpetrators of cybercrimes.

A 2021 report by Innovation for Poverty Action showed that 47% of Ugandans using digital financial services have faced attempted fraud through phone or SMS, while 33% have encountered phishing attempts. Even more concerning is that most incidents go unreported. The inadequacy of effective reporting of the cyber-crime criminals to police has proved to be a visible valid challenge.

According to the 2023 Uganda Police Force Annual Crime Report, it showed that only 245 cybercrimes were reported and of the UGX 1.5 billion lost to cybercrime, only UGX 377.4 million was recovered. Digital scams particularly target our most vulnerable populations, who often lack digital literacy skills. When these citizens fall victim to fraud, they are not just losing money but with it, faith in the formal financial system is lost, and many retreat to cash-based transactions and informal saving methods. This ultimately perpetuates financial exclusion.

The requirement for regular license renewals and subscriptions for most software protection constitutes a significant, costly barrier in Uganda. While software protection pricing varies, the typical annual cost for basic antivirus defense alone falls roughly between USh 80,000 ($22.84) and USh 180,000 ($51.39). This financial reality means that a large portion of cyberspace users in Uganda simply cannot manage the necessary charges. Moreover, many organizations and individuals find it difficult to sustain the costs required to maintain an adequate standard of cyber security defense. As a direct result of these exorbitant

expenses, numerous organizations and private citizens in Uganda are compelled to leave their personal data security to chance.

Corruption understood as the abuse of entrusted power for personal benefit—remains one of the most pressing social and political challenges of our time due to its far-reaching effects on society and national stability. In Uganda, corruption within law enforcement is widespread, with bribery and impunity occurring frequently. When the justice system is compromised in this way, the public can no longer rely on prosecutors or judges to uphold their duties. Much of this misconduct among police and judicial officers stems from chronic institutional underfunding and inadequate salaries. As a result, even when officials are known to be involved in organized criminal activities, they are seldom investigated, significantly weakening the effectiveness of law enforcement.

Conclusion

Cybercrime in both countries has grown increasingly sophisticated, revealing major gaps in legislation, enforcement, and public awareness. Although laws such as Uganda's Computer Misuse Act (2011, amended 2022) and Indonesia's Electronic Information and Transactions Law provide a foundation, their effectiveness is undermined by weak institutional capacity, limited digital literacy, high security costs, and persistent corruption. The rising number of cyber incidents and financial losses demonstrates both the expanding opportunities for offenders and the inadequacy of current deterrence efforts. Because many cybercrimes are transnational, stronger domestic enforcement must be complemented by wider public education and deeper regional and international cooperation. An effective response therefore requires legal reform, enhanced forensic and investigative capacity, and strengthened institutional integrity. Ultimately, technological tools alone are insufficient; combating cybercrime demands systemic reforms and coordinated cross-border strategies, including harmonized legal frameworks, intelligence sharing, and collaborative action against offenses such as financial fraud and online trafficking.

Acknowledgment

This project has been funded with support of the ministry of education, culture, research and technology of republic of Indonesia. This publication/communication reflects the view only of the author and the ministry of education, culture, research and technology of republic of Indonesia cannot be held responsible for any use which may be made of the information contained therein.

References

1. BBC News. (2025, January 20). *Ugandan women trafficked to Dubai in sex exploitation network investigation.* BBC Africa Eye. https://www.bbc.com/news/world-africa
2. Badan Siber dan Sandi Negara (BSSN). (2019). *Laporan tahunan statistik keamanan siber nasional 2019.* https://bssn.go.id
3. CIO World Asia. (2024, August 23). *Indonesia hit by massive data breach affecting 4.7 million civil servants.* https://www.cioworldasia.com
4. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention).* Budapest: Council of Europe.
5. Detikcom. (2024, August 23). *Data 4,7 juta ASN BKN bocor, dijual di forum hacker.* https://news.detik.com

6. DetikFinance. (2024, August 24). *Hacker 'TopiAx' klaim jual data ASN di dark web.* https://finance.detik.com
7. Econstor. (2020). *Indonesia cybersecurity threat landscape report 2020.* Econstor Research Repository. https://www.econstor.eu
8. E-Journal UMM. (2021). Analisis ancaman dan serangan siber di Indonesia tahun 2019. *Jurnal Teknologi Informasi, 13*(2), 77–90. https://ejournal.umm.ac.id
9. Global Initiative Against Transnational Organized Crime (GI-TOC). (2023). *Global organized crime index 2023 — East Africa assessment.* Geneva: GI-TOC. https://globalinitiative.net
10. Harian Jogja. (2024, August 24). *Kebocoran 4,7 juta data ASN terungkap, dijual di dark web.* https://www.harianjogja.com
11. Jakarta Post. (2024, August 26). *Fresh data breach puts pressure on government to form cyber privacy agency.* https://www.thejakartapost.com
12. Otoritas Jasa Keuangan (OJK). (2025). *Laporan Indonesia Anti-Scam Center (IASC): Penanganan pengaduan penipuan online 2024–2025.* https://www.ojk.go.id
13. Otoritas Jasa Keuangan (OJK). (2025). *Rekapitulasi pengaduan IASC bulanan: Januari–Mei 2025.* Jakarta: OJK.
14. PricewaterhouseCoopers Uganda (PwC). (2024). *Project Tai: Information systems audit report.* Kampala: PwC Uganda.
15. Republic of Indonesia. (1999). *Law No. 36 of 1999 on Telecommunications.*
16. Republic of Indonesia. (2002). *Law No. 19 of 2002 on Copyright.*
17. Republic of Indonesia. (2008). *Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law).*
18. Republic of Indonesia. (2014). *Law No. 35 of 2014 on Child Protection.*
19. Republic of Indonesia. (2016). *Law No. 19 of 2016 amending Law No. 11 of 2008 on ITE.*
20. Republic of Indonesia. (2022). *Law No. 27 of 2022 on Personal Data Protection (PDP Law).*
21. Republic of Uganda. (2011). *Computer Misuse Act 2011.*
22. Republic of Uganda. (2022). *Computer Misuse (Amendment) Act 2022.*
23. Reuters. (2025, February 6). *Uganda charges finance ministry officials over $21 million theft from central bank.* https://www.reuters.com/world/africa
24. The Star. (2024, August 25). *Hacker selling Indonesia civil servants' data on dark web.* https://www.thestar.com.my
25. Uganda Communications Commission (UCC). (2024). *Annual communication sector report 2023/24.* Kampala: UCC.
26. Uganda Police Force. (2024). *Annual crime report 2023–2024: Cybercrime division.* Kampala: UPF.
27. United Nations. (1948). *Universal Declaration of Human Rights (UDHR).* New York: United Nations.
28. United Nations Office on Drugs and Crime (UNODC). (2023). *Cyber-enabled crime and human trafficking report.* New York: UNODC.
29. World Bank. (2024). *IDA country financial management review: Uganda 2023/24.* Washington, D.C.: World Bank.