Library Progress International *Print version ISSN 0970 1052*
Vol.45, No.2, Jul-Dec 2025: P.464-475 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Cyber Sextortion: An Emerging Threat To Netizens

Dr. Murangira B. Thierry

Senior Lecturer at the Kigali Independent University, Rwanda
thierrybm_murangira@yahoo.com

How to cite this article: Dr. Murangira B. Thierry (2025). Cyber Sextortion: An Emerging Threat To Netizens. Library Progress International, 45(2), 464-475

Abstract:
Sextortion is a form of online blackmail where perpetrators use sexually explicit material to extort victims. It is a growing cyber-enabled crime that uses digital technologies to coerce individuals into sharing sexual content or favors under threats of exposure. This article explores the issue in Rwanda, a country experiencing rapid digital growth yet facing gaps in digital literacy against this threat.

Between 2018 and 2024, the Rwanda Investigation Bureau recorded 59 sextortion cases, increasing annually by 16.6%. Victims were mainly women (87.7%) and youth aged 16–30 (49.2%), while most perpetrators were men aged 31–40 (54.9%).

The study identifies three forms of sextortion: financial (69.5%), involving monetary extortion; emotional, often by ex-partners for revenge or control; and opportunistic, where online predators exploit trust. These forms highlight the intersection of gender, age, digital exposure, and socio-economic vulnerability.

Despite advancements in cybersecurity, Rwanda's legal response remains inadequate, as sextortion straddles both conventional criminal offenses and cybercrime. The absence of specific legal provisions, combined with limited public awareness and digital skills, fuels underreporting and victimization. The article calls for a holistic strategy, including clearer legal frameworks, digital safety tools, public education, and coordinated stakeholder engagement.

Recognizing sextortion as both cybercrime and abuse of power, the study emphasizes the need for context-specific, rights-based solutions to protect vulnerable groups. Comprehensive interventions are essential to ensure a safer and more accountable digital space in Rwanda and similar settings.

Key Words: Sextortion, digital literacy, cyber-enabled crime, Netizen

INTRODUCTION

The rapid advancement of technology and the internet has transformed how people communicate, interact, and share information. While this digital revolution has created vast opportunities, it has also facilitated new forms of crime. Among the most pervasive and emerging of these is sextortion; a cyber-enabled offense that exploits personal vulnerabilities for financial gain, coercion, or other malicious purposes.

Sextortion involves the use of sexually explicit material, often obtained through deception or coercion, to blackmail individuals. It is a complex offense that frequently intersects with various legal provisions, including blackmail, cyberstalking, the publication of pornographic or indecent images, and corruption. Although it is primarily characterized by coercion through sexually explicit content, its multifaceted nature makes it difficult to categorize under a single legal definition.

In Rwandan legal system, despite significant progress in strengthening cybersecurity, sextortion presents a unique and evolving challenge. Victims often suffer in silence due to fear, stigma, and limited awareness, which in turn makes it difficult to accurately assess the scale of the problem. Compounding this issue is the limited research on sextortion within the Rwandan legal context, leaving critical gaps in understanding its prevalence, perpetrators, and victims.

Rwanda's legal framework addresses various aspects of sextortion through multiple laws; however, there is currently no comprehensive legal provision that explicitly defines or targets sextortion as a distinct offense. This legal ambiguity complicates both enforcement and the protection of victims. While the existing approach to criminalizing sextortion through related legal provisions has proven somewhat useful, the author argues that there is still no clear consensus on the

most effective path forward whether to enact a specific law tailored to sextortion or to amend the existing law on the prevention and punishment of cybercrimes in order to address the gaps and challenges more effectively.

This article seeks to analyze the prevalence of sextortion in Rwanda, offering critical insights into its scope and legal treatment, while proposing practical legal solutions to mitigate its effects and enhance its prevention.

RESEARCH OBJECTIVES

This research aims to analyze the prevalence and nature of sextortion cases in Rwanda, identify the socio-demographic characteristics of both victims and perpetrators, and assess the legal framework in place to address this issue. Additionally, it seeks to propose effective legal strategies for prevention and response, including awareness campaigns, legal reform recommendations, and technological innovations to combat sextortion more effectively.

RESEARCH QUESTIONS

a. What is the extent and nature of sextortion in Rwanda?
b. Who are the primary victims and perpetrators, and what methods are commonly used?
c. How effective are legal responses to sextortion?
d. What measures can be adopted to mitigate the threat of sextortion in Rwanda?

RESEARCH METHODOLOGY

This research adopted doctrinal methods that will help to analyze reported and investigated cases on sextortion from Rwanda Investigation Bureau in the fiscal year 2018-2024 and document analysis to review of existing legal frameworks related to cybercrime and sextortion in Rwanda and in other developed countries including USA, UK, Singapore and South Africa.

LITERATURE REVIEW

Understanding Sextortion

Sextortion is a form of online blackmail where perpetrators use sexually explicit material to extort victims. The material may be real, fabricated, obtained through deceit or hacking. Perpetrators threaten to release this content to the victim's family, friends, or the public unless their demands are met.[1]

It is a form of technology-enabled crime where perpetrators coerce victims into performing specific actions usually providing money, explicit images, or videos by threatening to expose private or sensitive content of sexual nature. It is a blend of sexual exploitation and extortion, often executed through online platforms like social media, messaging apps, or email.[2]

Victims are often manipulated into sharing explicit content through deceitful relationships or are unknowingly recorded via electronic devices. Once in possession of compromising material, the perpetrators leverage fear, shame, and the threat of public exposure to control their victims.

Many countries have incorporated provisions into their national laws to address sextortion. The United Nations Children's Fund (UNICEF) defines "sextortion" and "sexual extortion of children" as the act of coercing a child into creating online sexual material by threatening to expose them.[3]

Sextortion a type of corruption

The International Association of Women Judges (IAWJ) defines sextortion as "the abuse of power to obtain a sexual benefit or advantage," framing it as a distinct form of corruption in which sex, rather than money, becomes the currency of the bribe.[4]

According to IAWJ, for an act to qualify as sextortion, two key components must be present. First is the sexual component, which encompasses any implicit or explicit request to engage in unwanted sexual activity not limited to intercourse but also including exposing private body parts, demanding explicit images or pornography, and unwanted physical contact. Second is the corruption component, whereby the individual making the request occupies a position of authority and

[1] Sextortion, a form of cyber-enabled crime, has emerged as a significant threat in the digital era. It involves coercing individuals to share sexually explicit images or videos, often through blackmail or manipulation. With the proliferation of technology and the rise of artificial intelligence (AI), sextortion has become more sophisticated, making it a pressing issue for individuals, law enforcement, and policymakers.

[2] FBI- What is sextortion? -Available at https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion, visited on 20 January, 2025.

[3] Transparency International: Criminalising Sextortion: Challenges and Alternatives, 2022. Available at: https://knowledgehub.transparency.org/assets/uploads/kproducts/Criminalising-sextortion_final_10.06.2022.pdf?utm_source=chatgpt.com. Visited on visited 30 Jan, 2025.

[4] The International Bar Association: Sextortion: A Crime of Corruption and Sexual Exploitation, 2019, London EC4A 4AD, United Kingdom, p 9

abuses that power to secure a sexual benefit in exchange for performing a duty. This corruption element is characterized by three features: an abuse of authority[5] (using a position of power for personal gain), a quid pro quo arrangement (demanding or accepting sexual favors in exchange for withholding or conferring a benefit), and psychological coercion (exerting pressure through threats or blackmail).[6]

Sextortion occurs when those entrusted with power exploit the dependency of others by leveraging their authority to obtain sexual benefits, which aligns with Transparency International's definition of corruption as "the abuse of entrusted power for private gain." In many instances, the quid pro quo is not a freely negotiated exchange but a scenario in which victims comply to avoid penalties or harsher treatment, effectively receiving no benefit but merely avoiding a disadvantage. For instance, in Kenya, a police officer was prosecuted for demanding sexual favors from female drivers in lieu of fines a case classified as abuse of power and corruption rather than extortion.[7]

Sextortion as Blackmail

Sextortion as blackmail occurs when an individual threatens to disclose explicit images, videos, or other sensitive content unless the victim complies with demands typically for money, more explicit content, or other favors. The key elements of sextortion include coercion, the threat of exposure, and non-consensual demands.

From a legal perspective, in some jurisdictions; this form of sextortion is classified either under criminal blackmail, extortion, or cyber-enabled crime laws. In the U.S., extortion statutes (18 U.S.C. § 875(d)) criminalize threats to harm a person's reputation or disclose compromising materials for financial or personal gain. Similarly, in Singapore, Sections 383–389 of the Penal Code define extortion as using fear to compel someone to surrender property or security.[8] A notable example is the Ogoshi brothers' sextortion case in the U.S., where Nigerian scammers targeted young victims, threatening to release explicit images unless a ransom was paid tragically leading to severe consequences.[9]

The author contends that sextortion can be understood through two distinct legal and conceptual lenses: as blackmail, typically involving cyber threats and image-based coercion and as corruption, where authority figures abuse power to solicit sexual favors. While both forms involve coercion and power imbalances, they differ in legal treatment, the actors involved, and contextual settings. Despite increasing international awareness, many countries lack specific laws addressing sextortion, often relying on broader statutes like bribery or sexual exploitation. This dual character of sextortion highlights the urgent need for tailored legal frameworks and coordinated efforts to protect victims and ensure justice.

Sextortion in Different Jurisdictions

- **Acts of Sextortion in Singapore**

Sextortion, a form of cybercrime involving coercion through threats of exposing explicit images or videos, has become an emerging concern in Singapore. Victims are often lured through social media or dating platforms, where perpetrators manipulate them into compromising situations. This issue highlights the sophistication of modern scams and the significant threats posed by cyber exploitation. Singapore has established strong legal frameworks to combat sextortion. Under the Penal Code, several provisions apply to such crimes.

Section 503 on Criminal Intimidation[10] criminalizes threatening another person with injury to their person, reputation, or property, intending to cause alarm or compel them to act against their will. Sextortion cases often involve such threats to reputation. Extortion, covered under Sections 383 to 389, defines the crime as inducing fear of injury to obtain money or valuables applicable when perpetrators demand payment in exchange for not exposing explicit content.[11] Additionally, "distribution of intimate images" is defined under Section 377BE. This provision criminalizes the threat to distribute intimate images or recordings without consent, knowing it will cause humiliation, alarm, or distress. This directly pertains to sextortion cases involving threats to release explicit content.[12]

Sextortion is classified as a cyber-enabled crime in Singapore, meaning it involves traditional criminal offenses facilitated through digital platforms. The Singapore Police Force (SPF) distinguishes between cyber-dependent crimes (such as hacking) and cyber-enabled crimes (such as sextortion, which leverages online platforms for exploitation). To strengthen

[5] IAWJ, Stopping the Abuse of Power through Sexual Exploitation: Naming, Shaming, and Ending Sextortion (2012)

[6] The International Bar Association: Sextortion: A Crime of Corruption and Sexual Exploitation, 2019, London EC4A 4AD, United Kingdom, p 9

[7] Kenya Anti-Corruption and Economic Crimes Act (2003)

[8] Singapore Penal Code (Sections 383–389)

[9] U.S. Extortion Law (18 U.S.C. § 875(d)),

[10] Criminal Intimidation: Penalties for Making Threats in Singapore: https://singaporelegaladvice.com/law-articles/criminal-intimidation-illegal-to-threaten-to-beat-someone/ visited on 21 February, 2025.

[11] Penal Code 1871 - Singapore Statutes Online. Available at: https://sso.agc.gov.sg/Act-Rev/PC1871/Published/20081130?DocDate=20081130&ProvIds=pr383-. Visited om 21 February, 2025

[12] Cybersexual Crimes in Singapore and Their Penalties: Available at https://singaporelegaladvice.com/law-articles/cybersexual-crimes-singapore-penalties/ visited on 21 February, 2025.

legal protections, Singapore has introduced measures like the Online Criminal Harms Act, reinforcing efforts to prosecute offenders and safeguard individuals from online exploitation.[13]

Therefore, while sextortion utilizes digital platforms, it is prosecuted under existing provisions of the Penal Code addressing extortion and intimidation. This issue has gained prominence as perpetrators exploit social media and dating platforms to lure victims into compromising situations. The Singapore Police Force (SPF) actively addresses this threat through awareness campaigns, urging victims to report incidents via dedicated hotlines and online platforms. Educational initiatives emphasize safe online practices, such as avoiding interactions with strangers on dating apps and safeguarding personal information

- **Acts of Sextortion in United States of America**

In the United States of America, the Federal Bureau of Investigation (FBI) describes sextortion as "a crime that happens online when an adult convinces a person who is younger than 18 to share sexual pictures or perform sexual acts on a webcam" It follows a more literal understanding, which combines extortion and sexual circumstances.[14]

In the U.S., while there is not a federal statute explicitly labeled "sextortion", such offenses are prosecuted under existing laws related to extortion, child exploitation, and cybercrimes. For instance, cases involving minors often fall under federal child pornography statutes, which criminalize the production, distribution, and possession of explicit images of minors. Additionally, the federal extortion statute (18 U.S.C. § 875) addresses threats made through interstate communications, including those involving coercion for sexual favors or images. Notably, some states have enacted specific laws targeting sextortion; for example, South Carolina's[15] "Gavin's Law" makes sextortion a felony, named after a teenager who tragically took his own life after being victimized.[16]

- **Recent Sextortion Cases in the U.S. Resulting in Deaths**

Several recent sextortion cases in the United States have resulted in tragic deaths, highlighting the severe impact of this cyber-enabled crime. In one case, a Nigerian national was extradited to the U.S. for his involvement in a sextortion scheme that led to the death of a South Carolina teenager. In a separate incident, an Ivory Coast man was charged in connection with a scheme that resulted in the suicide of a North Dakota teenager. In 2024, Nigerian brothers, Samuel and Samson Ogoshi were sentenced to lengthy prison terms for their sextortion plot, which led to the suicide of a Michigan teenager. Other significant cases include a Mississippi man charged with targeting over 40 victims, a Virginia man sentenced to three years for a scheme affecting over 100 young female victims, and a Columbus man who received more than four years in prison for sextorting young gay men on dating apps. Additionally, a man from Turks and Caicos was arrested for sextorting a Missouri teenager, and four Delaware men were charged in an international sextortion and money laundering operation.[17] In response, authorities, including the FBI and U.S. Attorney's Office, have issued public advisories to raise awareness about the risks of sextortion, particularly among teenagers. These cases highlight the urgent need for stronger prevention measures, legal enforcement, and international cooperation to combat sextortion.[18]

- **Acts of Sextortion in United Kingdom**

The United Kingdom's National Crime Agency (2021) defines sextortion as "a form of webcam blackmail, where criminals befriend victims online by using a fake identity and persuade them to perform sexual acts in front of their webcams". Sextortion is prosecuted under existing laws pertaining to blackmail and sexual offenses. The Sexual Offences Act 2003 criminalizes various forms of sexual exploitation, and the offense of blackmail under the Theft Act 1968 is often

[13] In Singapore, cybercrime is categorized into two clusters of crimes: Cyber-dependent Crime: Offences under the Computer Misuse Act (CMA) in which the computer is a target. This includes offences such as ransomware, hacking and website defacements. Cyber-enabled Crime: Offences in which the computer is used to facilitate the commission of an offence. Examples of cyber-enabled crime include online scams and cyber extortion, and other Penal Code offences committed via an online medium. Available at https://www.police.gov.sg/Advisories/Crime/Cybercrime. Visited on 21 February, 2025.

[14] Federal legislation in the United States also uses sextortion in this meaning, as found, for example, in the Trafficking Victims Protection Act of 2017 and the Missing Children's Assistance Act of 2018.

[15] United States Attorney's Office – District of South Carolina: Nigerian Man Extradited to the U.S. After Being Indicted for Sextortion Scheme that Caused Death of S.C. Teen. Available at: https://www.justice.gov/usao-sc/pr/nigerian-man-extradited-us-after-being-indicted-sextortion-scheme-caused-death-sc-teen Visited 30 Jan, 2025.

[16] The Federal Criminal Code (18 U.S.C. § 2251) includes penalties for extortion involving sexually explicit images of minors. The Cybersecurity and Infrastructure Security Agency (CISA) has also initiated awareness campaigns against sextortion.

[17] United States Attorney's Office – District of South Carolina: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion visited 30 Jan, 2025.

[18] The FBI has seen a huge increase in the number of cases involving children and teens being threatened and coerced into sending explicit images online—a crime called sextortion. Available at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion/sextortion. Visited on 20 April, 2025

applied in sextortion cases. The National Crime Agency (NCA) has been proactive in issuing warnings and working to combat the rise of sextortion cases, emphasizing the serious nature of these offenses and the potential for extradition of perpetrators operating from abroad.[19]

- **Acts of Sextortion in South Africa**

South Africa addresses sextortion through its anti-corruption and sexual offense laws. The Prevention and Combating of Corrupt Activities Act criminalizes abuse of power for any form of gratification, which can encompass demands for sexual favors. Additionally, the Sexual Offenses Act includes provisions against sexual exploitation and abuse. However, challenges remain in prosecuting sextortion due to evidentiary issues and the need for victims to come forward.[20]

- **Acts of Sextortion in Rwanda**

Act of sextortion in Rwanda legal system is primarily qualified as an act of blackmail and is prosecuted as one rather that corruption. Sexual related corruption acts are prosecuted under corruption law.[21] This approach aligns with the country's legal framework, which addresses abuses of power for personal sexual gain because the conduct constitutes an abuse of entrusted power for private gain, fitting squarely within Rwanda's anti-corruption law.

In this regard, the author argues that both sextortion and sex-based corruption constitute forms of abuse of power, though they occur in different contexts and involve distinct power dynamics. Both rely on coercion and exploitation, rooted in an imbalance of power where authority or influence is used to obtain sexual favors. However, they diverge in terms of context and methods of coercion. Sextortion typically occurs in digital spaces and involves threats to expose intimate content, whereas sex-based corruption usually takes place in person and is linked to official positions or benefits. While sextortion employs blackmail such as threats to release private material sex-based corruption relies on inducement or the abuse of authority, for example, demanding sexual favors in exchange for employment or advancement.

Sextortion as a Multi-Faceted Crime

In Rwanda, sextortion is a complex offense that often intersects with multiple legal provisions. While it is primarily characterized by coercion using sexually explicit material, it may also involve blackmail, cyber-stalking, publication of pornographic or indecent images and corruption. Rwanda's legal framework addresses different aspects of sextortion through various laws, but there is no single, comprehensive provision explicitly defining it.

- **Revenge Pornography and Sextortion**

Sextortion closely intersects with legal provisions governing the publication of pornographic or indecent material. When perpetrators threaten and releases sexual images or videos, they violate laws protecting individual privacy and dignity. If such material is non-consensually disseminated, additional charges related to revenge pornography or unauthorized publication may apply.

Article 34 of the Law on Prevention and Punishment of Cybercrimes criminalizes the distribution of pornographic content,[22] including child pornography, through digital means. Sextortion often involves perpetrators obtaining or manipulating explicit images and using them as leverage to coerce victims. When minors are involved, the crime may escalate to child exploitation, making this provision particularly relevant. However, this provision applies in cases where a perpetrator, after the victim refuses to comply, proceeds to publish explicit images or videos as an act of retaliation.

Similarly, Article 38[23] of the same law extends liability to individuals who publish or transmit indecent content online. Since sextortionists frequently use digital platforms to threaten or share compromising material, this provision becomes applicable when such threats are carried out. Like article 34, it also covers instances where perpetrators retaliate against victims who refuse to comply with their demands by disseminating explicit content.

- **Cyberstalking as Sextortion**

[19] National Crime Agency, 'Sextortion (webcam blackmail)' (National Crime Agency, 2019) https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-andextortion/sextortion-webcam-blackmail. Visited 15 July, 204.

[20] Transparency International: Criminalising sextortion: challenges and alternatives, 2022. Available at: https://knowledgehub.transparency.org/assets/uploads/kproducts/Criminalising-sextortion_final_10.06.2022.pdf?utm_source=chatgpt.com. Visited on visited 30 Jan, 2025.

[21] Article 6 Law on Law N° 54/2018 of 13/08/2018 fighting against corruption, prosecutes anyone who requests, accepts, or demands sexual favors in exchange for providing or withholding a service commits an offense. Official Gazette No. Special of 20/09/2018.

[22] Publication of pornographic images through a computer or a computer system is criminalized under Law N° 60/2018 of 22/8/2018 on prevention and punishment of cybercrimes. Official Gazette No. Special of 27/09/2018.

[23] Publishing indecent information in electronic form. Official Gazette No. Special of 27/09/2018.

Another legal element closely related to sextortion is cyberstalking. It refers to the persistent and malicious tracking of an individual online. Perpetrators often gather personal information about their targets to manipulate, intimidate, or harm them. This behavior frequently serves as a precursor to more severe offenses, such as blackmail and sextortion.

Article 35 of the Law on Prevention and Punishment of Cybercrimes specifically addresses cyberstalking,[24] which encompasses online harassment, threats, and the unauthorized distribution of intimate images. Since sextortion often involves persistent stalking behavior where perpetrators repeatedly harass victims through threats of exposure or coercion for additional explicit content. The provision on cyberstalking is crucial in prosecuting sextortion cases where digital threats and harassment are involved.

Perpetrators exploit hacked material or images obtained maliciously or shared in confidence to control and manipulate victims. In the digital realm, this often includes intimate photos and various forms of online harassment, such as sending threatening messages, sharing non-consensual images, or orchestrating cyberbullying campaigns to force compliance.

These actions not only escalate the psychological impact on victims but also create intersections with other crimes, including cyberstalking and blackmail. By leveraging intimidation and digital surveillance, perpetrators systematically erode victims' autonomy, making cyberstalking a critical element in the broader context of sextortion-related offenses.

- **Blackmail as an Element of Sextortion**

Article 129 on blackmailing[25] criminalizes using threats to obtain money, assets, or signatures by damaging a person's reputation. Sextortion falls within this category when perpetrators demand money or other benefits in exchange for not releasing content of sexual nature by any means. However, blackmail laws do not fully encompass cases where the demand involves sexual favors instead of financial or material gain.

- **Sextortion as a Form of Corruption**

Article 6 on soliciting or offering sexual favors[26] criminalizes the demand for sexual favors in exchange for services or benefits. The author asserts that this provision is particularly relevant in cases of sextortion where an individual secretly records explicit videos or images during such encounters and later uses them to threaten their superior, coercing them into compliance. In this scenario, sex serves both as a form of bribery and a means of blackmail, ultimately resulting in corruption-based sextortion.

- **Sextortion as Hybrid Offences**

This crime typically begins with the acquisition of compromising material, whether through consensual sharing, deceit, or hacking. Because sextortion commonly occurs via digital platforms, categorizing it solely as a cybercrime may heighten both its legal and moral implications. While it overlaps with traditional blackmail, its classification as a cybercrime becomes particularly significant due to the misuse of technology and potential violations of laws governing obscene or pornographic content.

Technology as an Enabler of Sextortion

The author argues that what sets sextortion apart from extortion and traditional blackmail is the role of technology in both facilitating and amplifying the crime. Perpetrators exploit social media, messaging platforms, and even artificial intelligence to create, obtain, or manipulate content of sexual nature. Additionally, the internet provides anonymity, allowing offenders to target victims across borders with minimal fear of immediate consequences.[27]

The key distinction in sextortion lies not in the threat itself but in the nature of the content and the heightened online humiliation inflicted on victims. At its core, sextortion is a form of blackmail a long-established crime in which threats are used to extort money, favors, or concessions through sexual images. The coercive element, specifically the threat of exposing compromising content, aligns precisely with the legal definitions of blackmail under Rwandan law[28]. In this

[24] Cyberstalking is addressed under Law N° 60/2018 of 22/8/2018 on prevention and punishment of cybercrimes. Official Gazette No. Special of 27/09/2018.

[25] Law N°68/2018 of 30/08/2018 determining offences and penalties in general. Official Gazette No. Special of 27/09/2018.

[26] Law N° 54/2018 of 13/08/2018 on Fighting Against Corruption. Official Gazette No. Special of 20/09/2018.

[27] Kareem, Karwan Mustafa. "Guardians of Anonymity: Exploring Tactics to Combat Cyber Threats in Onion Routing Environments." arXiv preprint arXiv:2406.07563 (2024). The author analyzes how onion routing networks, designed to protect user privacy, are exploited by cybercriminals for illegal activities, highlighting the challenges in tracing illicit actions due to the strong anonymity these networks provide.

[28] Article 129 of law N°68/2018 of 30/08/2018 determining offences and penalties in general, defines blackmail as an act of using threats to force someone into signing documents, revealing secrets, or handing over money or assets. Whether based on truth or lies, it's a criminal offense. Upon conviction the offenders face 1 to 3 years in prison and fines between 100,000 Frw and 300,000 Frw. If the threats are carried out, penalties increase to 3 to 5 years in prison and fines of up to 2,000,000 Frw.

context, the author argues that, the use of technology should lead to sextortion being redefined as a purely cybercrime rather than a traditional form of blackmail, as digital tools significantly expand its reach, scale, and impact.

Difference Between Extortion, Sextortion and Sexual-related Corruption

To understand the difference between sextortion and sexual-related corruption, it is essential to first distinguish among extortion, sextortion, and sexual related offenses. Extortion under Rwandan law ,[29] involves coercing someone to give money, property, or services through threats of future harm and is prosecuted under law determining offences and penalties in general. Sextortion,[30] while not explicitly defined in Rwandan law, is treated as a form of blackmail.[31] It involves using sexually explicit material often obtained through deceit to threaten victims into providing money, more explicit content, or sexual favors. This crime occurs primarily online and reflects a blend of digital blackmail and coercion.

Sexual-related corruption,[32] on the other hand, refers to situations where individuals in positions of authority demand sexual favors in exchange for services or benefits, rather than monetary bribes. This constitutes a form of corruption under Rwandan anti-corruption laws, as it involves the abuse of power for personal, non-financial gain.

The key legal distinctions are; extortion seeks material gain; sextortion leverages explicit content, often online, for similar ends; and sexual-related corruption involves power abuse, with sex as the currency of corruption. Sextortion, though often prosecuted as blackmail, encompasses elements of cybercrime and sexual exploitation, making it a complex offense that merges traditional crime with digital tools. This cyber-enabled crime exploits online personal vulnerabilities for financial gain, coercion, or other malicious intents. However, defining sextortion as solely a blackmail oversimplifies its nature, modus operandi and context. Upon closer examination, the author opines that sextortion emerges as a multifaceted offense, combining elements of traditional crimes like blackmail with technology-enabled methods and offenses of cybercrimes that are related to the publication of pornographic or indecent materials as well as cyberstalking. Recognizing its full scope is critical for developing appropriate legal and policy responses.

DATA ANALYSIS AND INTERPRETATION

Sextortion, a serious form of exploitation, has emerged as a growing concern in Rwanda, with individuals increasingly targeted through both personal and anonymous online attacks. To better understand this escalating threat, the author analyzes data on suspect profiles and methods used, drawing from reported and investigated cases between July 2018 and June 2024. This data offers valuable insight into the patterns and trends of these offenses, which is essential for developing effective responses and preventive strategies.

Trend of Sextortion Cases in last 6 Fiscal Years 2018-2024

The trend of sextortion has seen significant fluctuations over the past six fiscal years (2018-2024),[33] as reflected in the data below, this growing cyber-enabled crime has had varying impacts annually, influenced by factors such as increased online activity, advancements in technology, and social media penetration, as well as heightened public awareness and law enforcement interventions. The total cases reported (2018–2024) are 59 with average annual increase approximately 16.6%. The highest number of cases in a single year: 14 cases (2019–2020 & 2023–2024), while the lowest number of cases are 4 cases (2018–2019).

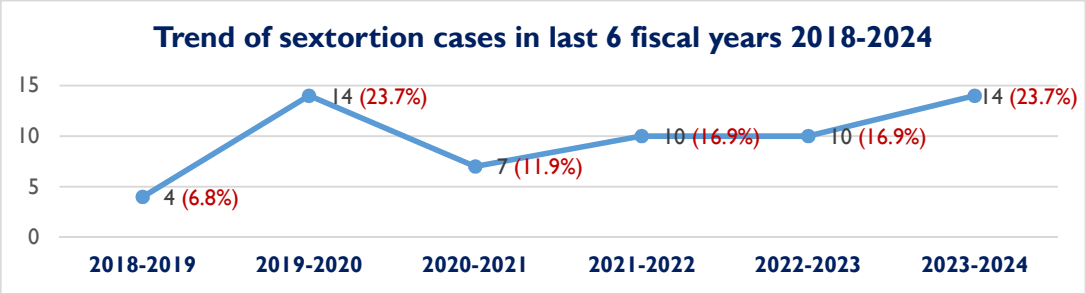
[29] Article 171 of law N°68/2018 of 30/08/2018 determining offences and penalties in general defines extortion to mean that anyone who uses violence or coercion to obtain a signature, fingerprint, or illicit gain from another person commits an offense. Official Gazette No. Special of 27/09/2018.

[30] As coined by FBI, Federal legislation in the United States also uses sextortion in this meaning, as found, for example, in the Trafficking Victims Protection Act of 2017 and the Missing Children's Assistance Act of 2018.

[31] Article 129 of law N°68/2018 of 30/08/2018 determining offences and penalties in general states that blackmail is the act of using threats to force someone into signing a document, accepting or denying responsibility, revealing a secret, or handing over money or assets. Whether the information is true or false, if it harms the victim's reputation or causes them distress. Official Gazette No. Special of 27/09/2018.

[32] Article 6 Law on Law N° 54/2018 of 13/08/2018 fighting against corruption, prosecutes anyone who requests, accepts, or demands sexual favors in exchange for providing or withholding a service commits an offense. Official Gazette No. Special of 20/09/2018.

[33] Source: Rwanda Investigation Bureau (2018–2024),



Over six fiscal years, sextortion cases showed a fluctuating yet upward trend, with notable spikes in 2020 and 2024. The data underscores the adaptive nature of cybercriminals and highlights the need for continuous investment in prevention, digital literacy, and enforcement strategies.

Victim-Suspect Demographics

The analysis of victim and suspect demographics in sextortion cases reveals significant trends in gender and age dynamics. Women overwhelmingly constitute the majority of victims (87.7%), suggesting that sextortion disproportionately affects females, likely due to societal factors that make them more vulnerable to online exploitation. Conversely, male victims (12.3%) remain a minority, but their presence highlights that sextortion is not exclusively a female-targeted crime. On the perpetrator side, men (76.1%) are the dominant offenders, reinforcing the trend that men are more frequently involved in digital exploitation, while female suspects (23.9%) also play a role, often through emotional or social manipulation.

Age-wise, the most targeted victims are young adults (16-30 years, 49.2%), who are highly active online and thus more susceptible to digital threats. Middle-aged adults (31-45 years, 32.3%) are also significantly affected, often due to professional or personal relationships. Victimization decreases with age, with only 1.5% of cases involving individuals over 61, reflecting lower digital engagement among older adults.

On the suspect side, the majority (54.9%) are aged 31-40, indicating that perpetrators are often individuals with greater technological proficiency and social manipulation skills. Younger suspects (21-30 years, 36.6%) are also prominent, showing that sextortion crimes are often committed by individuals familiar with online platforms. Offenders above 41 years are rare, likely due to reduced technological engagement.

In summary, the data underscores the intersection of digital access, gender, and age in sextortion cases. Women and young adults are the most affected, while perpetrators are predominantly middle-aged men. This highlights the need for targeted digital safety education, gender-sensitive legal frameworks, and stronger enforcement mechanisms to combat sextortion effectively.

Categories of Victims

The data presents categories of victims involved in sextortion cases, grouping them into different demographic or social categories such as people in relationships, professionals, young adults, adults, and minors/teenagers. **The data reveals that sextortion affects individuals across different age groups and professional backgrounds, with the most vulnerable groups being those in relationships, professionals, and young adults.**

People in Relationships (33.8%), the largest group, likely targeted due to the emotional leverage perpetrators can exploit through intimate content. Professionals (26.2%), a significant portion, potentially vulnerable due to the risks sextortion poses to their careers and reputations. Young Adults (23.1%), highly susceptible, as they are more active online and may be easily manipulated through digital platforms. Adults (13.8%), though a smaller group, middle-aged individuals can also be targeted, possibly due to their stable personal and professional lives. Minors and Teenagers (3.1%), a small but concerning percentage, showing that even younger individuals are not exempt from sextortion.

The findings highlight that sextortion primarily affects individuals in relationships, working professionals, and young adults, likely due to emotional vulnerability, online exposure, and reputational risks. Although minors represent a small portion, their presence underscores the wide-ranging impact of sextortion.

Category of Suspects

Based on data collected, perpetrators of sextortion can be categorized into five distinct groups. The largest category, comprising 49.3% of cases, consists of **scammers and fraudsters** who engage in sextortion as part of broader fraudulent schemes, primarily for financial gain. Following this, **former intimate partners** make up 22.5%, where individuals exploit past relationships for blackmail or revenge.

Similarly, **online predators** also account for 22.5% of cases. These perpetrators leverage online anonymity to manipulate and exploit victims into providing compromising materials. Another category, **catfishers,** represents 4.2%. These individuals create fake identities to build trust before ultimately deceiving and exploiting their victims.

The final and least common category consists of **organized criminal networks**, representing only 1.4% of cases. Though rare, these instances indicate that some sextortion schemes involve larger, coordinated efforts rather than individual perpetrators.

The data suggests that nearly half of the perpetrators are fraudsters, while former partners and online predators also account for a significant portion, highlighting the diverse motives behind sextortion.

Forms of Sextortion

The data highlights three primary forms of sextortion Financial Sextortion, Revenge Sextortion, and Romantic/Emotional Exploitation showing varying degrees of prevalence and impact.

From the data provided, **Financial Sextortion** is the most prevalent form, representing **69.5%**. This suggests that the majority of sextortion incidents involve individuals being targeted with demands for money, often under false pretenses such as the impersonation of someone known to the victim. This type of sextortion appears to be the most widespread, possibly because it exploits the victim's financial vulnerability.

Revenge Sextortion, which accounts for **18.6%**, is the second most common form that suggests that sextortion is also fueled by retaliation, often after relationship disputes. The misuse of explicit images shared in trust shows the risks of digital intimacy and personal conflicts escalating into coercion.

Finally, **Romantic or Emotional/Sexual Exploitation** accounts for **11.9%**. This form of sextortion involves the exploitation of emotional or romantic ties, where the victim is manipulated into performing sexual acts or providing intimate material based on a fabricated emotional connection. Though less frequent, it highlights the power of trust-based coercion, making victims less likely to recognize or report the abuse.

A critical conclusion drawn from this analysis is that financial gain is the primary driver of sextortion, reflecting a broader trend of monetizing personal exploitation. While revenge and emotional manipulation remain notable factors, the overwhelming dominance of financial sextortion suggests that perpetrators are increasingly treating it as a lucrative criminal enterprise. This highlights the urgent need for stronger legal and technological measures to combat sextortion and protect potential victims.

GENERAL CONCLUSION

The proportion of households owning mobile phones has risen significantly from 64% in 2014 to 85% in 2024. In urban areas, ownership increased from 89% in 2017 to 94% in 2024, while in rural areas, it grew from 62% in 2017 to 81% in 2024.[34] This rapid increase in mobile phone ownership, has expanded access to digital services but also heightens the potential exposure to cyber-related crimes such as sextortion, online fraud, identity theft, and digital scams. As mobile connectivity deepens, so does the need for comprehensive public awareness campaigns, robust cybersecurity measures, and legal frameworks to protect users and combat emerging digital threats.

Sextortion is a deeply invasive crime that thrives in the shadows of the digital world. Legal frameworks and awareness efforts are crucial in combating this menace. By leveraging laws, technology, and education, societies can work towards mitigating sextortion's impact and ensuring that the digital age remains a space for empowerment rather than exploitation. By safeguarding individual rights and promoting a culture of respect and accountability online, we can mitigate the impact of these crimes and uphold the principles of human dignity and justice.

Summary of Findings

The analysis of sextortion cases highlights critical trends in victimization, perpetration, and motivation. Women and young adults are the most vulnerable groups, with emotional leverage, online exposure, and reputational risks playing key roles in their victimization. The majority of perpetrators are middle-aged men, often engaging in fraudulent schemes or exploiting past relationships.

Financial sextortion dominates, accounting for nearly 69.6% of cases, underscoring the growing trend of monetizing personal exploitation. Revenge and emotional manipulation also play significant roles, though to a lesser extent. The data further suggests that professionals and individuals in relationships are at heightened risk, while organized criminal networks play a minor role in sextortion cases.

Ultimately, sextortion is a multifaceted crime driven primarily by financial motives, emotional control, and digital manipulation. Strengthening legal frameworks, enhancing digital literacy, and implementing proactive cybersecurity measures are essential in combating this growing threat.

Need for a Specific Provision on Sextortion

[34] The Seventh Integrated Household Living Conditions Survey (EICV7) was conducted from October 2023 to October 2024, published April, 2025. Available at: https://www.statistics.gov.rw/publication/eicv7-key-findings-booklet. Visited 24 April, 2025.

Sextortion is a relatively new term that highlights emerging crimes facilitated by digital communication and technology. It refers to a form of exploitation in which individuals are coerced into performing sexual acts or providing explicit images, often under threats of exposing sensitive material. Although widely recognized in media and public discourse, sextortion is not a legally defined term in most jurisdictions. Instead, such cases are prosecuted under existing laws related to blackmail, extortion, sexual exploitation, cybercrimes, or corruption.

Rwanda's legal framework addresses different aspects of sextortion through provisions on cybercrime, blackmail, and corruption. However, there is no standalone law that explicitly defines and criminalizes sextortion as a distinct offense in category of cybercrime. Victims often face overlapping crimes, such as cyberstalking, blackmail, distribution of pornographic image or obscene content and abuse of power, requiring legal authorities to apply multiple provisions to a single case. Establishing a specific legal provision for sextortion would enhance enforcement efforts, provide greater legal clarity and bridge the gap, ensuring more effective prosecution and victim protection.

RECOMMENDATIONS

The link between sextortion, blackmail, cyberstalking, and online harassment reveals the multifaceted nature of cyber-enabled human rights violations. Sextortion represents a growing challenge in Rwandan's digital landscape like any other place in the world, underscoring the importance of vigilance and preventive measures for all netizens. Addressing these crimes requires a holistic approach that combines robust legal frameworks, public awareness, and international collaboration.

The findings suggest an urgent need for:

Public awareness campaigns that aims at educating the public about common tactics used in sextortion. Enhanced cybersecurity measures that encourages individuals to safeguard personal information online and stricter regulations aiming at strengthening laws to deter perpetrators and protect victims. Sextortion in Rwanda reflects both personal betrayals and systemic exploitation. By addressing these challenges through collaboration between authorities, communities, and technology platforms, the fight against sextortion can gain significant momentum.

Digital literacy programs: To mitigate these risks, it is proposed that the government and relevant stakeholders invest in digital literacy programs tailored for both urban and rural populations, particularly targeting vulnerable groups.

Legal Reforms: Consider undertaking legal reform by amending the law on the prevention and punishment of cybercrimes to include a specific provision defining sextortion. This would help streamline the handling of such cases and enhance access to justice for victims.

Strengthening cybersecurity measures to protect individuals from online predators and scams and enforcing stricter regulations on digital service providers, and enhancing collaboration between law enforcement, telecom operators, and tech platforms are also critical steps toward ensuring a safe digital environment for all users.

Scope for Further Research

Due to limited data and legal ambiguity on sextortion in Rwanda, this study focuses primarily on a legal analysis. However, it highlights the need for future research to explore the psychological, social, and economic impacts on victims, including trauma and stigma.

Studies on unreported cases could reveal cultural and institutional barriers to reporting, while examining perpetrators' motivations could support prevention and rehabilitation efforts. Additionally, the role of technology in both enabling and preventing sextortion, especially among youth on social media, deserves further investigation. Exploring how gender norms affect vulnerability is also essential for a comprehensive national response.

REFERENCES

LEGAL FRAMEWORK

1. Budapest Convention on Cybercrime (2001)
2. Federal Criminal Code (18 U.S.C. § 2251)
3. Kenya Anti-Corruption and Economic Crimes Act (2003)
4. Law N° 54/2018 of 13/08/2018 on fighting against corruption
5. Law Nº 60/2018 of 22/8/2018 on prevention and punishment of cybercrimes
6. Law No. 60/2018 of 22/8/2018 on the Prevention and Punishment of Cybercrimes in Rwanda.
7. Law Nº68/2018 of 30/08/2018 determining offences and penalties in general
8. Penal Code 1871 - Singapore Statutes Online.
9. Singapore Computer Misuse Act (CMA)
10. U.S. Extortion Law (18 U.S.C. § 875(d)),
11. United Nations Convention on the Rights of the Child (1989)
12. US Trafficking Victims Protection Act of 2017 and the Missing Children's Assistance Act of 2018

CASE LAW

1. R v. George (UK, 2021)
2. United State of America v. Samuel Ogoshi, No 2.22-CR-25-RLL
3. United States of America v. Edell Jackson, No. 22-2870, 08 August, 2024
4. United States v. Vassiliadis (2018)
5. United States v. Woodbury (2:25-mj-02204) District Court, C.D. California
6. Unites States v. Lawal Hassanbunhussein AboloreEt Al, 0:23-cr-00850-CRI, 24 Oct, 2023
7. United States v. Jacob Rager, 2:25-cr-00021, Ohio Southern District Court, Feb 10, 2025
8. United States v. Omoruyi O. Uwadiae, 24-063, United States District Court Southern District of Ohio, 07 June, 2024
9. United States v.Tyler N. Grundstrom, 2:22-mj-01345, Dec 16, 2022

BOOKS

1. Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. ABC-CLIO.
2. Cybercrime: Criminal Threats from Cyberspace" by Susan W. Brenner, 2023
3. Furnell S. (2002). Cybercrime: Vandalizing the information society. Boston, MA: Addison-Wesley,
4. IAWJ, Stopping the Abuse of Power through Sexual Exploitation: Naming, Shaming, and Ending Sextortion (2012)
5. Sextortion: The Hidden Pandemic" by Emma-Jane Cross: This book delves into the psychological and societal impact of sextortion, exploring its prevalence and offering strategies for prevention.
6. Sherri Davidoff Et All, Cyber Extortion, Response and Prevention
7. The International Bar Association: Sextortion: A Crime of Corruption and Sexual Exploitation, 2019, London EC4A 4AD, United Kingdom, p 9

ONLINE ARTICLES

1. CEDAW, Article 1, https://www.un.org/womenwatch/daw/cedaw/text/econvention.htm.
2. Choi K. (2008). Computer crime victimization and integrated theory: An empirical assessment. International Journal of Cyber Criminology, 2, 308-333.
3. Council of Europe, Budapest Convention on Cybercrime, https://www.coe.int/en/web/cybercrime/the-budapest-convention.
4. Criminal Intimidation: Penalties for Making Threats in Singapore: https://singaporelegaladvice.com/law-articles/criminal-intimidation-illegal-to-threaten-to-beat-someone.
5. Cybersexual Crimes in Singapore and Their Penalties: Available at https://singaporelegaladvice.com/law-articles/cybersexual-crimes-singapore-penalties.
6. FBI- What is sextortion? -Available at https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion.
7. Hall, M. (2018). Digital Victimology. Springer. Journal of Cybersecurity Research, Volume 12, Issue 3, 2023
8. International Telecommunication Union (ITU). "Cybercrime and the Challenge of Online Privacy.
9. Kareem, Karwan Mustafa. "Guardians of Anonymity: Exploring Tactics to Combat Cyber Threats in Onion Routing Environments, 2024.
10. National Center for Missing & Exploited Children (NCMEC). "The Impact of Sextortion on Victims.
11. National Crime Agency, 'Sextortion (webcam blackmail)' (National Crime Agency, 2019) https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-andextortion/sextortion-webcam-blackmail.
12. Sextortion in the Digital Age: A Growing Threat to Privacy and Security", published in the Journal of Cybersecurity Research.
13. The Role of AI in Amplifying Sextortion Crimes" in Computer Law & Security Review.
14. Transparency International: Criminalising Sextortion: Challenges and Alternatives, 2022. Available at: https://knowledgehub.transparency.org/assets/uploads/kproducts/Criminalising-sextortion_final_10.06.2022.pdf?utm_source=chatgpt.com.
15. Transparency International: Criminalising sextortion: challenges and alternatives, 2022. Available at: https://knowledgehub.transparency.org/assets/uploads/kproducts/Criminalising-sextortion_final_10.06.2022.pdf?utm_source=chatgpt.com
16. United States Attorney's Office – District of South Carolina: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion.

17. United States Attorney's Office – District of South Carolina: Nigerian Man Extradited to the U.S. After Being Indicted for Sextortion Scheme that Caused Death of S.C. Teen. Available at: https://www.justice.gov/usao-sc/pr/nigerian-man-extradited-us-after-being-indicted-sextortion-scheme-caused-death-sc-teen.

RELEVANT PRESS RELEASE BY FBI ON CASES OF VICTIMS OF SEXTORTION

Press Release by FBI on Cases of victims of Sextortion: Available at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion/sextortion.

1. All Charged Money Launderers Tied to Nigerian Sextortion Scheme Plead Guilty released on 03 April,2025.
2. Columbus Man Pleads Guilty to Sextorting Minor Females Social Media, Possessing Child Pornography released on 28 February, 2025
3. Columbus Man Sentenced to More Than Four Years in Prison for Cyberstalking, Sextorting Young Gay Men He Targeted on Dating Apps released on 17 December, 2025
4. FBI Detroit Hosts Second Webinar in West Michigan Educating Community on Sextortion. released on 11 April, 2025
5. Ivory Coast Man Charged with Participating in a Sextortion Scheme That Caused the Death of a North Dakota Teenager released on 22 January, 2025
6. Jackson Man Pleads Guilty to Child Exploitation, Cyberstalking, and Sextortion Offenses release on 21 February, 2025.
7. Mississippi Man Charged in Sextortion Scheme Involving More Than 40 Victims released on 01 October, 2024
8. Money Launderer Tied to Nigerian Sextortion Scheme Pleads Guilty released on 22 January, 2025
9. Nigerian Man Extradited to the U.S. After Being Indicted for Sextortion Scheme That Caused Death of South Carolina Teen release on 27 January, 2025
10. Sextortionist Gets 24 Years for Victimizing Minors Online release on 21 February, 2025
11. Woodbury Man Pleads Guilty in Child Sextortion Scheme released on 25 March, 2025 03