Sustaining Digital Security: The Role of the Indonesian Cyber Police in Handling Sextortion Cases in Bangka Belitung

[1] Syafri Hariansah, [2] Misnah Irvita, [4] Yang Meiliana, [*5] Suriadi Sirait
[1-5] Faculty of Law, Universitas Pertiba

*Corresponding Author:
suriadisirait@gmail.com

Abstract

Digital security is a crucial element in ensuring a sustainable digital environment, particularly in addressing the growing threat of cyber crimes such as sextortion. Sextortion, a form of digital extortion, has become increasingly prevalent and requires effective law enforcement measures. This study aims to examine the role of the Indonesian Cyber Police (Siber Polri) in handling sextortion cases in Bangka Belitung, focusing on the effectiveness of enforcement strategies, challenges encountered, and innovations implemented. A qualitative research approach with descriptive analysis was employed, utilizing interviews with law enforcement officers, legal document analysis, and case studies of reported sextortion incidents. The findings indicate that while Siber Polri has integrated various digital investigation technologies, several challenges persist. These include the lack of specific regulations addressing sextortion, low digital literacy among the public, and difficulties in tracking perpetrators across multiple jurisdictions. To enhance the effectiveness of law enforcement efforts, this study suggests the implementation of more adaptive legal frameworks, the advancement of investigative technologies, and stronger collaboration among law enforcement agencies, digital service providers, and the community. A more innovative and adaptive approach by Siber Polri will contribute significantly to sustainable digital security and ensure better protection for society in the digital era.

Keywords: Digital Security, Cyber Police, Sextortion

I. INTRODUCTION

In the era of rapid digital transformation, cybersecurity has become one of the most crucial issues in maintaining public order and comfort in the digital space. The development of information technology has not only brought positive impacts in various aspects of life but has also presented serious challenges in the form of cybercrimes, one of which is sextortion. Sextortion is a form of extortion that uses sexual content as a means to threaten and extort the victim. This phenomenon knows no boundaries and can affect anyone, including communities in island regions like Bangka Belitung. The lack of digital literacy, insufficient understanding of personal data security, and weak monitoring of online activities exacerbate the vulnerability to such crimes.

In addressing these challenges, the presence and active role of Indonesia's Cyber Police are crucial. As part of law enforcement focusing on digital issues, the Cyber Police are not only tasked with handling cases after they occur but are also responsible for preventive efforts through education, monitoring, and strengthening reporting systems. In Bangka Belitung, handling sextortion cases requires an adaptive approach, considering the unique geographic and socio-cultural characteristics of the local community. The Cyber Police in this region must be able to collaborate with various stakeholders, such as government agencies, local communities, educational institutions, and non-governmental organizations, to create a safe and inclusive digital ecosystem.

This article aims to delve deeper into the role of Indonesia's Cyber Police in handling sextortion cases in Bangka Belitung. This study will explore the strategies that have been implemented, the challenges faced on the ground, and the effectiveness of the approaches used in addressing these cases. By understanding the local conditions and the dynamics of digital crimes in the region, it is hoped that this article can contribute to the development of more responsive and sustainable digital security policies. Additionally, the findings of this study are expected to serve as a reference for efforts to improve the capacity of law enforcement officers and digital literacy in the community in facing cybercrime threats in the future.

METHOD

This study employs a **mixed methods approach**, combining both qualitative and quantitative methods to obtain a comprehensive understanding of the role of the Indonesian Cyber Police in handling sextortion cases in Bangka Belitung. The qualitative approach is used to explore in depth the strategies, challenges, and practices implemented by law enforcement officers, while the quantitative approach supports the qualitative findings through statistical data on the number of cases, crime trends, and reporting and resolution rates.

Qualitatively, data were collected through in-depth interviews with key informants such as members of the cyber units at the district (Polres) and provincial (Polda) police departments in Bangka Belitung, local staff from the Ministry of Communication and Information (Kominfo), as well as representatives from NGOs or victim advocacy organizations. Semi-structured interviews were conducted to allow for a more flexible and context-sensitive exploration of issues. Additionally, document analysis was carried out on official police reports, cybersecurity-related regulations, and media publications concerning sextortion cases in the region. The qualitative data were analyzed using thematic analysis, identifying patterns and key themes that emerged from the interviews and documents.

Quantitatively, data were collected through secondary data sources from relevant institutions, including crime statistics from the police and Kominfo, as well as findings from digital literacy surveys. This quantitative data was analyzed using descriptive statistical techniques such as percentages, frequencies, and distribution graphs to illustrate trends in sextortion cases, reporting rates, and law enforcement responses. The combination of both approaches allows the researcher not only to describe how the cyber police operate but also to assess the extent of their impact on reducing sextortion cases and enhancing public safety in Bangka Belitung.

To ensure **validity and reliability**, data triangulation was applied by comparing information from multiple sources and different methodological tools. The data collection process was conducted over a two-month period, adhering to research ethics, including informed consent from participants and the confidentiality of respondent identities. With this mixed methods approach, the study aims to provide a holistic picture and serve as a strong foundation for developing effective policies and practices in the handling of sextortion at both local and national levels.

RESULTS AND DISCUSSION

A. General Overview of Sextortion Cases in Bangka Belitung

Based on data from the Special Criminal Investigation Directorate (Ditreskrimsus) of the Bangka Belitung Regional Police between 2021 and 2023, at least 37 sextortion cases were officially reported by the public. The majority of victims were teenagers aged 14–20 years, who were active on social media platforms such as Facebook, Instagram, and WhatsApp. Perpetrators often disguised themselves as peers, establishing online relationships before manipulating victims into sharing intimate content, which was then used for extortion purposes. Approximately 76% of these cases were not reported to the authorities until victims experienced severe psychological distress or significant financial loss. This highlights the low level of digital literacy and reluctance to report among the population, especially in rural areas.

Geographically, the highest concentration of cases occurred in urban areas such as Pangkalpinang and Sungailiat, although a rising trend has also been observed in rural regions. According to interviews with local cyber police officers, limited access to forensic technology and a shortage of specialized personnel at the regional level present major challenges in addressing these cases. Furthermore, many victims are reluctant to report due to feelings of shame, fear of social exclusion, and lack of trust in the legal system.

B. Cyber Police Response Strategies

The cyber police in Bangka Belitung have implemented several strategies to combat sextortion cases. These include the formation of a **Cyber Patrol Unit** that actively monitors suspicious online activities on social media and local digital platforms. This unit collaborates with telecommunications operators and internet service providers to trace perpetrators through digital footprints and IP addresses. In cross-border cases, cooperation with Interpol and social media platforms is initiated to deactivate offenders' accounts. Interview findings indicate that in 87% of investigated cases, the perpetrators were successfully identified, although legal proceedings are often hampered by incomplete or deleted digital evidence.

On the **preventive side**, the cyber police, in partnership with the local Communication and Information Office (Kominfo) and educational institutions, have launched digital literacy programs and public campaigns under the themes **#BeraniLapor** (Dare to Report) and **#JagaPrivasi** (Protect Your Privacy) to raise awareness among the youth about the dangers of sharing personal data. However, evaluations of these programs reveal that their reach remains limited to major cities and has not been effectively extended to rural villages.

C. Field Challenges and Dynamics

Observations and interviews reveal several key challenges in the handling of sextortion cases in Bangka Belitung:

1. **Limited Technical Resources**: Digital forensic facilities are centralized at the national level, causing delays in evidence collection and analysis at the regional level.
2. **Legal and Jurisdictional Constraints**: Some cases are difficult to process as perpetrators use fake identities or operate from foreign countries, complicating jurisdiction.
3. **Victim Silence Culture**: Many victims remain silent due to fear of being blamed or socially stigmatized, which worsens their trauma and reduces the likelihood of legal recovery.

D. Evaluation and Implications for Digital Security

Despite progress in detection and investigation, the response efforts have not yet fully established a secure digital ecosystem in Bangka Belitung. A synthesis of the qualitative and quantitative findings suggests that repressive strategies must be balanced with continuous **preventive and educational approaches**. The cyber police require ongoing training, improved support infrastructure, and strong coordination systems with local governments and the private sector to enhance cybercrime response capabilities.

These findings are consistent with the study by **Chatterjee et al. (2018)**, which emphasized that successful responses to sextortion depend heavily on cross-sector collaboration and active community engagement. Moreover, law enforcement efforts should adopt a **victim-centered approach** to prevent re-victimization and build public trust in the justice system.

Table 1. Number of Sextortion Cases in Bangka Belitung (2021–2023)

Year	Number of Reported Cases	Average Age of Victims	Percentage of Resolved Cases
2021	9	18 years	55%
2022	12	17 years	67%
2023	16	16 years	75%
Total	**37**	—	—

Source: Ditreskrimsus Polda Kep. Bangka Belitung, 2023

Table 2. Key Challenges in Handling Sextortion Cases Based on Interviews

No	Challenge Category	Summary Description
1	Technical Resources	Limited availability of digital forensic tools at the regional level.
2	Regulation & Jurisdiction	Difficulty tracking perpetrators across regions or countries.
3	Victim Silence Culture	Victims are reluctant to report due to shame or fear of social stigma.
4	Limited Digital Education	Digital literacy programs have not yet reached rural communities equitably.

No	Challenge Category	Summary Description
5	Inter-agency Coordination	Insufficient synergy between police, Kominfo, and victim support organizations.

Source: Researcher Interviews with Cyber Police and Community Partners, 2024

Conclusion

Based on the findings of this study, sextortion cases in Bangka Belitung show a significant prevalence, with the majority of victims being teenagers who are active on social media. Although the local cyber police have made various efforts to address this issue, several challenges—including limited technical resources, difficulties in tracking perpetrators across borders, and a prevailing culture of silence among victims—hinder the overall effectiveness of case handling. Therefore, in addition to the repressive measures undertaken by law enforcement, **preventive efforts through education and increased digital literacy** are crucial to sustainably combat sextortion. A strong collaboration between government sectors, private institutions, and the public must be reinforced to build a secure and trustworthy digital ecosystem for the future.

Acknowledgements

The author would like to express sincere gratitude to the **Special Criminal Investigation Directorate (Ditreskrimsus) of the Bangka Belitung Regional Police**, who provided essential data and insights regarding sextortion cases in the region. Special thanks are also extended to the cyber police officers, the Communication and Information Office (Kominfo), and educational institutions who contributed their perspectives and valuable information through interviews that enriched this study. Finally, the author appreciates the community members who shared their experiences and reflections on the social and psychological impacts of this cybercrime.

Research Novelty

This study presents several novel contributions to the existing literature on digital security in Indonesia. First, it sheds light on the **specific dynamics of sextortion cases in Bangka Belitung**, a region that has rarely been highlighted in cybercrime research. Second, it identifies **technical and cultural challenges** that influence the handling of sextortion cases, focusing particularly on the limitations of regional digital resources and the social impacts experienced by victims. Third, the findings emphasize the importance of **victim-centered approaches** and **cross-sector collaboration**, offering fresh insights for the development of more effective cybercrime prevention policies and programs. Through this research, it is hoped that more **innovative and integrated steps** will emerge to mitigate the threat of sextortion in Indonesia.

Berikut adalah versi **terjemahan bahasa Inggris** dari daftar pustaka Anda, disusun secara profesional sesuai standar akademik internasional:

REFERENCES

1. Chatterjee, S., Das, A., & Nandi, S. (2018). *Cybercrime and Cybersecurity: Trends, Issues, and Countermeasures*. Springer.
   This book provides insights into the evolution of cybercrime and various efforts to combat it, including the role of cyber police in addressing cases such as sextortion.
2. Turelli, T., & Rogers, A. (2020). Digital Literacy and Cybersecurity in Emerging Economies: A Case Study of Indonesia. *International Journal of Cybersecurity, 18*(4), 251–265.
   This article discusses the level of digital literacy in Indonesia and how it affects society's capacity to respond to cybercrime threats, including sextortion.
3. Ministry of Communication and Information Technology of the Republic of Indonesia (Kominfo). (2022). *Cybercrime and Information Technology Utilization Report in Indonesia 2022*. Jakarta: Kominfo.
   This report provides statistics on the rise of cybercrime in Indonesia and outlines the government's strategies to address it.
4. Susanto, H. (2021). Cybercrime in Indonesia: Legal and Technological Approaches to Tackling Sextortion. *Indonesian Law Journal, 12*(2), 45–60.
   This article examines how Indonesia's legal system addresses sextortion and the use of technology in cybercrime investigations.
5. Aji, D. (2020). Digital Forensics in Indonesia: Challenges and Solutions in Cyber Crime Investigation. *Journal of Digital Forensics, Security and Law, 15*(3), 128–142.
   This study offers insights into the challenges faced by Indonesian authorities, including limitations in digital forensic tools and procedures when handling cybercrime cases like sextortion.
6. Rahmawati, F., & Setiawan, B. (2019). Digital Education and Cybercrime Prevention in Indonesia: The Role of Cyber Police in Sextortion Prevention. *Journal of Digital Communication and Security, 5*(1), 23–36.
   This research emphasizes the importance of digital education programs and the role of cyber police in combating crimes such as sextortion, particularly in rural areas.
7. Bangka Belitung Regional Police. (2023). *Annual Report on Cybercrime and Sextortion Offenses in Bangka Belitung*. Pangkalpinang: Special Criminal Investigation Directorate (Ditreskrimsus), Bangka Belitung Police Department.
   This police report provides updated data on sextortion cases in the region, serving as a primary source for this research.
8. Widodo, S. (2017). *Policing the Digital Age: The Role of Cyber Police in Indonesia*. *Indonesian Journal of Law and Society, 8*(3), 301–314.
   This book provides an in-depth analysis of the role of cyber police in Indonesia in facing digital crime threats and their adaptation to technological developments.
9. Cahyana, F., & Yuliana, P. (2020). Cybersecurity Policy in Indonesia: Between Regulation and Implementation. *Journal of Public Policy, 18*(4), 79–92.
   This article discusses Indonesia's cybersecurity policies, including regulations and programs for preventing and handling cybercrime, as well as implementation challenges at the regional level.

10. Joffe, A., & Lim, S. (2019). Sextortion: A Global Challenge in the Digital Era. *Journal of International Cyber Law and Policy,* *7*(2), 93–108. This article provides a comprehensive overview of sextortion as a global phenomenon, including case studies from Indonesia and recommendations for victim-centered approaches to tackle this crime.