Al-Ishlah: Jurnal Ilmiah Hukum
P-ISSN: 1410-9328 || E-ISSN: 2614-0071
https://jurnal.fh.umi.ac.id/index.php/ishlah/article/view/v27n1-2

Vol. 27 Issue 1: December 2023 - May 2024 Published Online: March 17, 2024

Article Title

Challenges of Hybrid Policing in Countering Online Fraud Networks: A Case Study from Sidrap Regency

Author(s)

I. G. N. Adi Suarmita[Ω]
Sekolah Tinggi Ilmu Kepolisian

Hadi Purnomo
Sekolah Tinggi Ilmu Kepolisian

[Ω]Correspondence Email
ngurahsuar44@gmail.com

How to cite:

Suarmita, I. G. N. A., & Purnomo, H. (2024). Challenges of Hybrid Policing in Countering Online Fraud Networks: A Case Study from Sidrap Regency. *Al-Ishlah: Jurnal Ilmiah Hukum, 27*(1), 17-30. https://doi.org/10.56087/aijih.v27i1.442

ABSTRACT

This research aims to examine the concept of hybrid policing in the context of crime prevention, specifically cyber fraud in Sidrap Regency. This research uses an empirical legal research method. All collected data is then qualitatively analyzed to describe the problem and answer the research objectives. The results show that the characteristics of cyber fraud in Sidrap Regency exhibit anonymity and disregard for geographical boundaries, with the primary motivation of the perpetrators being personal gain. They employ fake identities and compromised devices to execute their schemes, exacerbated by technological advancements, the public's lack of awareness, and existing regulatory gaps. Therefore, it is recommended that the POLRI renew and adapt their policing model to be more responsive to the dynamics of cybercrime by implementing a hybrid policing approach. This involves active collaboration with community organizations in prevention efforts, which are expected to increase public awareness and strengthen the cyber security network. Additionally, developing an effective knowledge management system is advised, facilitating the exchange of information and strategies for handling cybercrime cases more efficiently. For researchers, it is crucial to examine further the social and psychological impacts of cybercrime on victims, which can contribute to forming a theoretical and practical foundation for a more holistic and victim-oriented approach to preventing and handling cybercrime in Sidrap Regency.

Keywords: *Cybercrime, Hybrid Policing, Online Fraud.*

INTRODUCTION

Maintaining the Realization of Domestic Security is strongly influenced by various factors originating from within and outside the country. These dynamic conditions may turn into severe problems if not comprehensively anticipated. The rapid development of information and communication technology has had an impact that can divide society, although, on the other hand, these developments can facilitate people's lives (Oktana et al., 2023). A survey showed that using information and communication technology is dominant in Indonesia, with around 70% of the total population being 230 million (Alvara Research Center, 2020). Unwise use of information and communication technology has triggered various problems, including violating people's privacy by insults or unlawful acts (Prince et al., 2024).

Along with the development of information technology in the era of the Industrial Revolution 4.0, it has led to a new order of society. The main feature of this industrial revolution is the merging of information and communication technology in the industrial field with the emergence of the Internet of Things (IoT), big data, 3D printing, artificial intelligence (AI), and cloud computing (Rane, 2023). These conditions have led to increased internet usage in Indonesia. Another survey also shows that internet users in Indonesia reached 215.63 million people in the 2022-2023. This number increased by 2.67% compared to the previous period, which had 210.03 million users. The number of internet users equals 78.19% of Indonesia's population of 275.77 million. Compared to the previous period survey, Indonesia's internet penetration rate this year has increased by 1.17 percent compared to 2021-

2022, which was 77.02%. For information, the trend of internet penetration in Indonesia is increasing from year to year. In 2018, internet penetration in the country reached 64.8%, which rose to 73.7% in 2019-2020 (APJII, 2023).

The rapid development of digital media in Indonesia has created challenges in the form of higher rates of lawbreaking. Cybercrime increased significantly (up to 14 times) in 2022 compared to the same period in the previous year. From the beginning of the year until the 22nd of December in 2022, data on the e-MP of the State Police of the Republic of Indonesia[1] recorded that they cracked down on 8,831 cybercrime cases. All working forces in the Criminal Investigation Agency of POLRI[2] and Regional Police[3] in Indonesia prosecuted cybercrime cases. POLDA Metro Jaya is the working force with the highest number of prosecutions against such cases (3,709 cases). Meanwhile, in the same period in 2021, across Indonesia, only 26 working forces prosecuted a total of 612 cases (Pusiknas Bareskrim Polri, 2023).

Indonesia's cybercrime rate is ranked second in the world after Ukraine, with about 239.74 million cyberattacks recorded throughout 2021 (Fitra, 2022). According to the National Cyber and Encryption Agency, DKI Jakarta is the country's main cyberattack target. The number of cyberattacks directed at the Indonesian capital was recorded at 49.04 million times in 2021, followed by Aceh with 46.13 million cyberattacks, then West Java with 39.62 million cyberattacks, and there were also cyberattacks on Central Java and East Java 22.4 million times and 19.9 million times, respectively (Kominfo, 2015).

Several regional police forces, such as POLDA East Kalimantan, POLDA Metro Jaya, POLDA East Java, POLDA South Sumatra, and even POLRI, arrested several perpetrators from Sidrap Regency in 2021. Based on data from POLRI in 2021, around 70 people from the Regency were arrested. During that year, the Sidrap Police Resort[4] alone was only able to uncover 14 criminals, with victims spread across Central Sulawesi, West Java, South Sumatra, East Nusa Tenggara, Jakarta, Madura, North Maluku, and South Sulawesi. However, in further interrogation of the suspects, the number of victims totaled 75 people, and only two people reported against the group's modus operandi. From there, it appears that there are still around 73 people who are reluctant to report the fraud incident.

Cyber fraud is a crime committed in an internet network-based system that aims to deceive or manipulate information to gain as much profit as possible (Cross, 2022). Sidrap Regency was chosen as the location of this research because many cases occur in Indonesia of people who come from the Regency, and the worst thing is that

[1] Hereinafter referred to as the POLRI.
[2] Hereinafter referred to as the Bareskrim POLRI.
[3] Hereinafter referred to as the POLDA.
[4] Hereinafter referred to as the POLRES.

some cases are found by families who protect the perpetrators, even though they know that it is against the law. Because they feel protected by their surroundings, the perpetrators feel less and less afraid or hesitant to commit crimes. The unique nature of online crime is that it does not involve physical loss; in other words, the surrounding environment is not disturbed and instead impacts improving the economy of the family and the surrounding environment (Givens, 2023). Moreover, in its implementation, the perpetrator is not alone but together with his network, which generally comes from the people around him.

The network of online criminals in its implementation is not alone but divides its respective roles. According to Spaulding (1948), criminal networks are defined as a pair of relatively stable emotional ties between people, disciplined communication channels capable of transmitting information and emotions where they are freely bound between members of society. The concept of an illegal goods network or syndicate by Trocki (1987) states that there is agreement between views on illegal syndicates. A syndicate is generally run by two or more participants for profit-making activities, mostly material (earning money). Of course, the parties involved in the network have everyday needs, but these needs are not necessarily the same. Vold (1979) explains that organized crime has certain forms, such as syndication, extortion, political bribery, and corruption. Crime syndicates are a relatively stable type of business organization. The business organization integrates and coordinates criminal opportunities, criminal activities, and personnel in various tasks that guarantee greater profits. This condition can significantly impact the community, territory, and even country.

Fraud in the cyber world is the leading choice of criminals because it does not involve physical activity, and the lack of deterrent effects in the cyber world (Mohit, 2022). The deterrent effect in question is the activeness of the police in responding to the prevention of cybercrime and the community's antipathy towards cyber fraud criminals. As a result of the rise of online fraud crimes and the fact that Sidrap Regency Police have difficulty reaching crimes that occur in cyberspace, the community there is increasingly reluctant to report them. As a result, online fraud is proliferating in the Regency. The handling of cybercrime, in this case, cyber fraud, will be increasingly broad and complex, so it is necessary to increase the ability of the police to overcome it. The police are no longer passively waiting for reports but can act proactively, predictively, and holistically using technology. Policing that needs to be done is an effective one that can be done in cyberspace, namely hybrid policing (Laksana, 2003). Efforts to enforce cyber fraud should be one of the priorities of the POLRI. The need for online media users to feel safe in transactions and protected from all forms of deception is one of the human rights that every citizen must obtain or enjoy (Zainuddin & Salle, 2022).

Based on the description above, this research aims to examine the concept of hybrid policing in the context of crime prevention, specifically cyber fraud in Sidrap Regency. This objective is grounded in the understanding that hybrid policing can effectively combat cybercrime, yet it faces significant challenges in its implementation. The expected benefit of this research is to provide new insights into crime prevention strategies that can be adapted and applied in hybrid policing and to offer recommendations for overcoming obstacles in its application, thereby enhancing the effectiveness of cybercrime mitigation in Sidrap Regency.

METHOD

This research uses an empirical legal research method. This research seeks to comprehend legal practices as a social phenomenon by analyzing facts or data (Qamar & Rezah, 2020). It examines how various social, economic, political, psychological, and anthropological factors influence community behavior (Irwansyah, 2020). It utilizes both primary and secondary data sources. Data collection is conducted through interviews with key informants, field observations, the literature study technique, and document analyses of cyber fraud cases in Sidrap Regency. All collected data is then qualitatively analyzed to describe the problem and answer the research objectives (Sampara & Husen, 2016).

RESULTS AND DISCUSSION

A. Network Anatomy of Cyber Fraud in Sidrap Regency

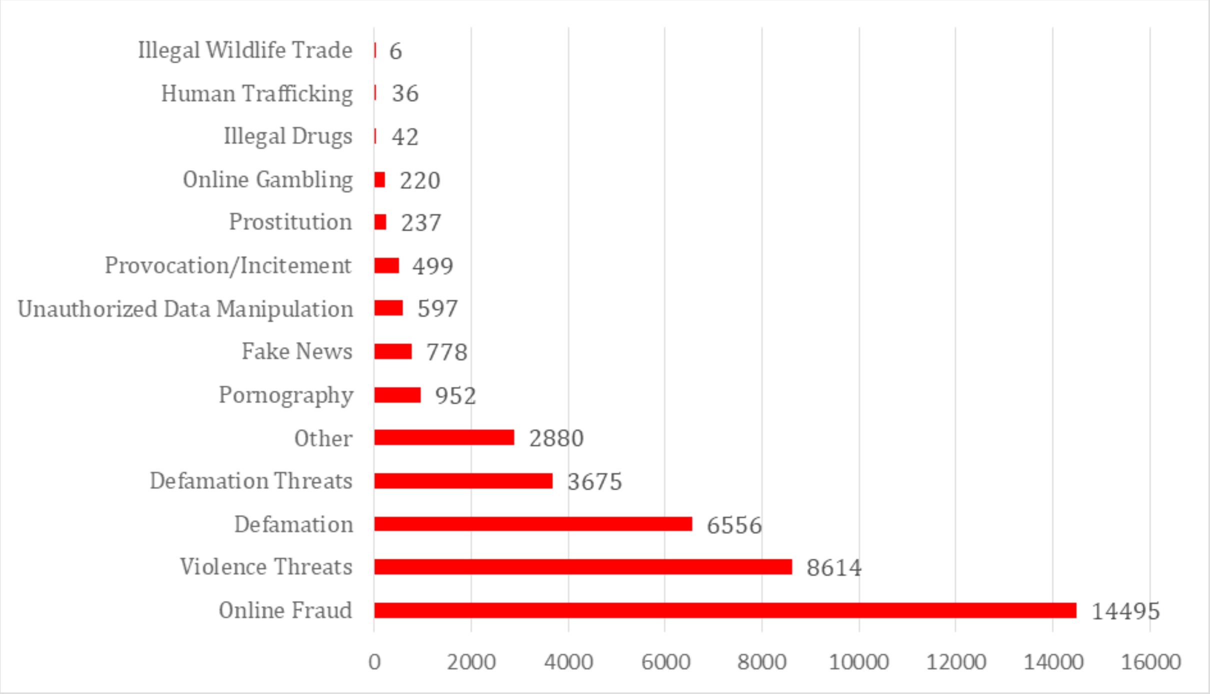
The government has made various efforts to handle cybercrime through the establishment of the Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (Id-SIRTII/CC) and the E-Commerce Task Force as a place for reporting people who are victims of fraud to be followed up (Solim et al., 2019). In addition, online fraud handling activities are under the objectives of Article 3 of Law Number 8 of 1999. Meanwhile, online fraud handling activities must refer to Law Number 11 of 2008[5]. These conditions have been implemented and applied at POLRES Sidrap through operational functions in criminal investigation and have been implemented comprehensively by all members with the hope of consistently protecting the public from cyber fraud. Nevertheless, cybercrime is still rampant in Indonesia, especially in that Regency.

The Ministry of Communications and Informatics recorded 1,730 online fraud content from August 2018 to February 2023, resulting in losses of IDR 18.7 trillion during 2017-2021. Based on research by the Center for Digital Society,

[5] Law Number 11 of 2008 has been amended more than once (Law Number 19 of 2016 for the first amendment; Law Number 1 of 2024 for the second amendment).

Gadjah Mada University, on 1,700 respondents in 34 provinces, 66.6% have been victims of online fraud. The mode details include 36.9% under the guise of gifts, 33.8% using links, 29.4% buying and selling fraud through social media, 27.4% through fake websites or applications, and 26.5% fraud under the guise of a family crisis. Most online fraudsters use SMS/phone calls (64.1%), followed by social media (12.3%), conversation apps (9.1%), websites (8.9%), and email (3.8%) (Septiani, 2023).

Figure 1.Cybercrime Case Content Report until March 2024



Source: Indonesian Cyber Patrol (2024)

One case of online fraud in Sidrap Regency involved several perpetrators. They share tasks: some send broadcast messages, some take calls or act as operators, and some print fake transfer receipts and pretend to be bank representatives. Then there is a 'boss' - who manages the bank account to receive the proceeds (money) from the ensnared victims. He is also the one who sets up all the necessary facilities and monitors the activities of the executors. The research found that rationalization is a critical element of many online fraud cases in and from Sidrap Regency; in other words, perpetrators seek justification for their crimes - whether for the necessities of life or the difficulty of finding a job. Some perpetrators consider the likelihood of being caught by law enforcement to be low due to the ease of manipulating identities in cyberspace. In addition to the perceived difficulty of being traced by the police, online fraud perpetrators also feel they can make huge gains with little investment. Studies show online fraudsters only need laptops, mobile phones, and USB modems. Through these devices, they create fake accounts and carry out their crimes. Interestingly, these devices do not have to be sophisticated or brand new as long as they are still functional and easy to tinker with.

The expected utility principle explains that people will make rational decisions based on the degree to which they expect to maximize gains or benefits and minimize losses or costs (Ingarasi & Suwigno, 2022). This rational choice theory also prioritizes how people fulfill their needs, including prestige, romance, and joy (Kaiser & Leeson, 2023). All of these elements influence a person's decision to behave. This theory was also found to contribute the most to the emergence of cyber fraud in Sidrap Regency, be it based on personal needs (perpetrators), the needs of their lovers, or even family needs, which are also one of their rationalizations. Need implies a state of deprivation, such as hunger or thirst, or essential things, such as refuge, safety, or cognitive and social stability. These needs are fundamental to any individual's well-being. Satisfying a need can mean more than simply reacting to a biological or psychological deficiency.

Based on research findings, it can be seen that the modus operandi of the perpetrators is very diverse. It starts from simple things like buying and selling goods to amorous relationships. At least four modus operandi of online fraud are found in this research. First, romance scam, where the victim is seduced and invited to have a serious romance, even to the point of being lured into marriage, and then blackmailed by utilizing the victim's love and sympathy. Second, email spoofing, where the victim is not careful and does not confirm with the producer regarding money transfers. Third, email fraud is when fake promotions or offers, usually job offers, tempt the victim: fourth, fraud in buying and selling goods with tempting promotions. Cyber fraud can be committed by someone from a very private place (e.g., a bedroom) but can cause harm to someone or an institution elsewhere, separated by distance, often even cross-border. As such, it may carry the nature of transnational crimes, i.e., crimes that cross territorial boundaries.

The overall analysis of the research shows that the perpetrators have calculated the risks of the goals they want to achieve. These considerations then influence the perpetrator to determine the actions and targets of the crime. Before acting, the perpetrator will make choices and determine decisions, which, in the process, are influenced by a set of factors. Cornish and Clarke (1986) describe a rational choice structure commonly found in cyber fraud in Sidrap Regency. First, the availability of targets and accessibility, where the perpetrators choose to use mobile phones with IMEI (International Mobile Equipment Identity) that are easily replaced as a means of carrying out their evil intentions. Second, awareness of the methods and skills needed; based on the facts obtained, these perpetrators learned how to commit fraud from friends who also committed the same crime.

Third, cash proceeds obtained per crime committed, the perpetrators carried out their actions against several victims at once, with the consideration that because the value was small (under Rp. 2,500,000), they felt that the police would not follow up on the crime. Fourth, done alone or with the help of others (if necessary), feeling supported, the perpetrators solidified their criminal intent. Fifth, the time taken to commit the crime, where they understood that they could commit fraud at any time. Sixth, if caught further, the severity of the punishment encourages their efforts to be anonymous online.

What is interesting about the findings of this research is that the perpetrators seem to understand the regulations and take advantage of the loopholes in them. They deliberately target victims outside South Sulawesi Province or Sulawesi Island, as if they know that fraud cases are guided by Supreme Court Regulation Number 2 of 2012. If the operational costs of police investigations from outside the jurisdiction exceed the loss suffered by the victim, the case is categorized as a minor crime. Even the chances of returning the victim's money are minimal, even though the perpetrator has been arrested.

The research explains that reporting cyber fraud still has a fundamental obstacle between reporting to the police or reporting it on the platform used. It was also mentioned that the reluctance to report is due to the psychological impact of reporting fraud but not getting clarity on the reporting results (Morrison et al., 2010; Fonseca et al., 2022). However, why do so many online fraud cases in Indonesia involve people from the Sidrap Regency? This article will be discussed further in the next section.

B. Challenges in Countering Cyber Fraud

Along with developing government services that utilize sophisticated technologies (commonly known as e-government), it also makes it a potential target for cyber attackers. Intrusions into e-government systems can occur at any time if not adequately secured. One study related to e-government security reported in 2005 that 82% of e-government sites worldwide were (still) vulnerable to cyber-attacks (Zhao & Zhao, 2010). Furthermore, in 2007, developed countries, especially the United States, became the target of the most cyber-attacks in the form of Denial of Service (DoS) attacks (Yaacoub et al., 2023).

If using the perspective that no system is immune, Indonesia certainly has the same vulnerability, or even more, considering that the nation is still in the absorption and adaptation stage regarding technology utilization. In implementing and strengthening the security of its electronic-based government system, according to Article 41 section (2) of Presidential Regulation Number 95 of 2018, these tasks are implemented by a particular institution engaged in cyber security.

It is in line with the literature that describes the consequences of the development of cybercrime, which has also led to the emergence of various policing practices and state-funded non-police organizations in cyberspace. However, it further explains that what has been done needs to be revised in controlling cybercrime due to a lack of training and understanding of the cybercrime phenomenon and contradictions in relevant policies and regulations.

The literature highlights the ideal policing model for dealing with cybercrime. These range from the implementation of military policing models that emphasize the adaptation of military technology and methods (Haggerty & Ericson, 2000), highlighting the importance of digital footprints (such as IP addresses and timestamps) (Huang & Wang, 2009), the reform of public policing, and the growth of the private security industry that creates plurality in law enforcement (Jones & Newburn, 2006), the need for policies that give police authority over Internet Service Providers (ISPs) (Kerr & Gilbert, 2004), the importance of international partnerships in cybercrime law enforcement especially in the context of Mutual Legal Assistance (MLA) (Broadhurst & Le, 2013) to proposing a shift from a reactive investigation model to a community policing model (Wall & Williams, 2007).

In the context of the role of specific institutions, actors, or agencies, some previous studies refer to it, such as highlighting the importance of engaging online communities in regulating and maintaining order in their domains while establishing virtual policing services alongside conventional policing services as a form of de-monopolization of policing functions (Matthies et al., 2012), research that resulted in a public/private policy combining private security roles with public security policing in China (Zhong & Grabosky, 2009), and studies that recognized the capabilities of police agencies, while promoting partnerships between stakeholders in cybercrime prevention, called multi-agency partnerships (Levi & Williams, 2013).

In this research, crime prevention should be the goal of policing models. The Indonesian government has been trying to address cybercrime, including online fraud, by developing a cyber policing model. However, POLRI faces several challenges in combating cyber fraud using a hybrid policing approach. These challenges include sectoral ego behavior among law enforcement officials, lack of public awareness about digital threats, absence of comprehensive cybersecurity regulations and standards, and legal loopholes that prevent effective deterrence of perpetrators. Furthermore, Indonesia's vast and archipelagic geography makes monitoring and controlling online fraud cases difficult (Widagso & Hariyani, 2016). Inadequate equipment, poor coordination between agencies, and a lack of proactive measures by local police also contribute to a weakened response and decreased public trust (Husen et al., 2020).

CONCLUSIONS AND SUGGESTIONS

Based on the results and discussions, it is concluded that the characteristics of cyber fraud in Sidrap Regency exhibit anonymity and disregard for geographical boundaries, with the primary motivation of the perpetrators being personal gain. They employ fake identities and compromised devices to execute their schemes, exacerbated by technological advancements, the public's lack of awareness, and existing regulatory gaps. This conclusion underscores the importance of enhancing public awareness and strengthening regulations as preventive measures.

Based on the conclusion above, it is recommended that the POLRI renew and adapt their policing model to be more responsive to the dynamics of cybercrime by implementing a hybrid policing approach. It involves active collaboration with community organizations in prevention efforts, which are expected to increase public awareness and strengthen the cyber security network. Additionally, developing an effective knowledge management system is advised, facilitating the exchange of information and strategies for handling cybercrime cases more efficiently. For researchers, examining the social and psychological impacts of cybercrime on victims is crucial, which can contribute to forming a theoretical and practical foundation for a more holistic and victim-oriented approach to preventing and handling cybercrime in Sidrap Regency.

REFERENCES

Alvara Research Center. (2020, December). *20/21: Tahun yang Mengubah Arah Peradaban Manusia* (Catatan Akhir Tahun). https://alvara-strategic.com/wp-content/uploads/2020/12/Catatan-Akhir-Tahun-Alvara-2020.pdf

Asosiasi Penyelenggara Jasa Internet Indonesia. (2023). *Hasil Survei Internet APJII 2023*. https://survei.apjii.or.id/survei/2023

Broadhurst, R., & Le, V. K. (2013). Transnational Organized Crime in East and South East Asia. In A. T. H. Tan (Ed.), *East and South-East Asia: International Relations and Security Perspectives* (pp. 223-235). Routledge.

Cornish, D. B., & Clarke, R. V. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Springer-Verlag.

Cross, C. (2022). Using Artificial Intelligence (AI) and Deepfakes to Deceive Victims: The Need to Rethink Current Romance Fraud Prevention Messaging. *Crime Prevention and Community Safety, 24*(1), 30-41. https://doi.org/10.1057/s41300-021-00134-w

Fitra, K. S. (2022, December 12). *Kerugian Akibat Kejahatan Siber di Dunia Tembus Rp129.643 Triliun*. Bisnis.com. Retrieved October 15, 2023, from https://teknologi.bisnis.com/read/20221212/84/1607768/kerugian-akibat-kejahatan-siber-di-dunia-tembus-rp129643-triliun

Fonseca, C., Moreira, S., & Guedes, I. (2022). Online Consumer Fraud Victimization and Reporting: A Quantitative Study of the Predictors and Motives. *Victims & Offenders, 17*(5), 756-780. https://doi.org/10.1080/15564886.2021.2015031

Givens, A. D. (2023). New Knowledge, Better Decisions: Promoting Effective Policymaking through Cybercrime Analysis. *International Journal of Cybersecurity Intelligence & Cybercrime, 6*(1), 1-4. https://doi.org/10.52306/2578-3289.1153

Haggerty, K. D., & Ericson, R. V. (2000). The Surveillant Assemblage. *The British Journal of Sociology, 51*(4), 605-622. https://doi.org/10.1080/00071310020015280

Huang, W., & Wang, S.-Y. K. (2009). Emerging Cybercrime Variants in the Socio-Technical Space. In B. Whitworth & A. d. Moor (Eds.), *Handbook of Research on Socio-Technical Design and Social Networking Systems* (pp. 195-208). IGI Global. https://doi.org/10.4018/978-1-60566-264-0.ch014

Husen, L. O., Salle, S., Syalman, A. A., & Muzakkir, A. K. (2020). Pengamanan Intelijen Kepolisian Terhadap Putusan Pengadilan Atas Objek Sengketa. *SIGn Jurnal Hukum, 1*(2), 136-148. https://doi.org/10.37276/sjh.v1i2.62

Indonesian Cyber Patrol. (2024, March). *Jumlah Laporan Polisi Yang Dibuat Masyarakat*. https://patrolisiber.id/statistic

Ingarasi, P., & Suwigno, N. P. (2022). The Benefits of Registered Trademark for MSME Actors in Surakarta City: A Case Study of IPR Protection. *SIGn Jurnal Hukum, 4*(2), 233-246. https://doi.org/10.37276/sjh.v4i2.187

Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Mirra Buana Media.

Jones, T., & Newburn, T. (Eds.). (2006). *Plural Policing: A Comparative Perspective*. Routledge. https://doi.org/10.4324/9780203001790

Kaiser, A. J., & Leeson, P. T. (2023). Why Rational Choice? Reconciling Kornai with Rational Choice Theory. *Acta Oeconomica, 73*(S1), 75-86. https://doi.org/10.1556/032.2023.00034

Kerr, I. R., & Gilbert, D. (2004). The Role of ISPs in the Investigation of Cybercrime. In T. Mendina & J. Brtiz (Eds.), *Information Ethics in an Electronic Age: Current Issues in Africa and The World* (pp. 163-172). McFarland Press. https://ssrn.com/abstract=907483

Laksana, C. D. (2003). Pemolisian Komuniti (Community Policing) dalam Menciptakan Keamanan dan Ketertiban Masyarakat. *Jurnal Polisi Indonesia, 4*(5), 6-25.

Law of the Republic of Indonesia Number 8 of 1999 on Consumer Protection (State Gazette of the Republic of Indonesia of 1999 Number 22, Supplement to the State Gazette of the Republic of Indonesia Number 3821). https://jdih.dpr.go.id/setjen/detail-dokumen/tipe/uu/id/409

Law of the Republic of Indonesia Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843). https://jdih.dpr.go.id/setjen/detail-dokumen/tipe/uu/id/138

Law of the Republic of Indonesia Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952). https://jdih.dpr.go.id/setjen/detail-dokumen/tipe/uu/id/1683

Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6905). https://jdih.dpr.go.id/setjen/detail-dokumen/tipe/uu/id/1842

Levi, M., & Williams, M. L. (2013). Multi-Agency Partnerships in Cybercrime Reduction: Mapping the UK Information Assurance Network Cooperation Space. *Information Management & Computer Security, 21*(5), 420-443. https://doi.org/10.1108/imcs-04-2013-0027

Matthies, C. F., Keller, K. M., & Lim, N. (2012). *Identifying Barriers to Diversity in Law Enforcement Agencies*. RAND Corporation. https://doi.org/10.7249/OP370

Ministry of Communications and Informatics of the Republic of Indonesia. (2015, 10 April). *Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber*. https://www.kominfo.go.id/index.php/content/detail/4698/Indonesia-Peringkat-ke-2-Dunia-Kasus-Kejahatan-Siber/0/sorotan_media

Mohit, S. G. (2022). Significance of Cyber Security in Cyber World. *International Journal of Advanced Research in Science, Communication and Technology, 2*(9), 49-53. https://doi.org/10.48175/ijarsct-5193

Morrison, G. R., Ross, S. M., Kemp, J. E., & Kalman, H. (2010). *Designing Effective Instruction* (Sixth Edition). John Wiley & Sons Ltd.

Oktana, R., Akub, S., & Maskun, M. (2023). Social Media in the Process of Evidence of Electronic Information and Transaction Crimes. *SIGn Jurnal Hukum, 4*(2), 320-331. https://doi.org/10.37276/sjh.v4i2.252

Presidential Regulation of the Republic of Indonesia Number 95 of 2018 on the Electronic-Based Government System (State Gazette of the Republic of Indonesia of 2018 Number 182). https://peraturan.go.id/id/perpres-no-95-tahun-2018

Prince, C., Omrani, N., & Schiavone, F. (2024). Online Privacy Literacy and Users' Information Privacy Empowerment: The Case of GDPR in Europe. *Information Technology & People, 37*(8), 1-24. https://doi.org/10.1108/itp-05-2023-0467

Pusat Informasi Kriminal Nasional Bareskrim Polri. (2023, 25 September). *Kejahatan Siber di Indonesia Naik Berkali-kali Lipat*. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV. Social Politic Genius (SIGn).

Rane, N. L. (2023). Integrating Leading-Edge Artificial Intelligence (AI), Internet of Things (IoT), and Big Data Technologies for Smart and Sustainable Architecture, Engineering and Construction (AEC) Industry: Challenges and Future Directions. *International Journal of Data Science and Big Data Analytics, 3*(2), 73-95. https://doi.org/10.51483/ijdsbda.3.2.2023.73-95

Regulation of the Supreme Court of the Republic of Indonesia Number 2 of 2012 on the Adjustment of Petty Crime Limits and the Amount of Fines in the Penal Code. https://jdih.mahkamahagung.go.id/legal-product/perma-nomor-2-tahun-2012/detail

Sampara, S., & Husen, L. O. (2016). *Metode Penelitian Hukum*. Kretakupa Print.

Septiani, L. (2023, February 24). *Kominfo Catatkan 1.730 Kasus Penipuan Online, Kerugian Ratusan Triliun*. Katadata.co.id. Retrieved October 15, 2023, from https://katadata.co.id/digital/teknologi/63f8a599de801/kominfo-catatkan-1730-kasus-penipuan-online-kerugian-ratusan-triliun

Solim, J., Rumapea, M. S., Wijaya, A., Manurung, B. M., & Lionggodinata, W. (2019). Upaya Penanggulangan Tindak Pidana Penipuan Situs Jual Beli Online di Indonesia. *Jurnal Hukum Samudra Keadilan, 14*(1), 96-109. https://doi.org/10.33059/jhsk.v14i1.1157

Spaulding, C. B. (1948). Cliques, Gangs and Networks. *Sociology and Social Research, 32*, 928-937.

Trocki, C. A. (1987). The Rise of Singapore's Great Opium Syndicate, 1840-86. *Journal of Southeast Asian Studies, 18*(1), 58-80. https://doi.org/10.1017/S0022463400001259

Vold, G. B. (1979). *Theoretical Criminology*. Oxford University Press.

Wall, D. S., & Williams, M. (2007). Policing Diversity in the Digital Age: Maintaining Order in Virtual Communities. *Criminology & Criminal Justice, 7*(4), 391-415. https://doi.org/10.1177/1748895807082064

Widagso, K., & Hariyani, O. S. (2016). Hybrid Policing as an Alternative Model of Policing Against Cybercrime in the Information Society. *Indonesian Journal of International Law, 13*(4), 577-597. https://doi.org/10.17304/ijil.vol13.4.670

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2023). Ethical Hacking for IoT: Security Issues, Challenges, Solutions and Recommendations. *Internet of Things and Cyber-Physical Systems, 3*, 280-308. https://doi.org/10.1016/j.iotcps.2023.04.002

Zainuddin, Z., & Salle, S. (2022). The Legal Awareness of Juveniles in Archipelagic Areas Using Social Media. *SIGn Jurnal Hukum, 3*(2), 163-173. https://doi.org/10.37276/sjh.v3i2.177

Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and Threats: A Security Assessment of State E-Government Websites. *Government Information Quarterly, 27*(1), 49-56. https://doi.org/10.1016/j.giq.2009.07.004

Zhong, L. Y., & Grabosky, P. N. (2009). The Pluralization of Policing and the Rise of Private Policing in China. *Crime, Law and Social Change, 52*, 433-455. https://doi.org/10.1007/s10611-009-9205-1