Available online at: http://jurnal.president.university.ac.id

PROBLEMATIKA HUKUM

| ISSN (Print) 2477-1198 | ISSN (Online) 2503-4812 |

ANALYSIS OF INFORMATION TECHNOLOGY CRIME AND CRIMINAL LAW ENFORCEMENT POLICY EFFORTS IN THE ERA OF GLOBALIZATION

Devinda S[1], Rizqyta P.K[2], Cindy Firdiani[3], Tomasia Da Costa[4], Shifa S.S[5], Chelsea Z.P.G[6]

[1]*Faculty of Law, President University, Indonesia. E-mail: devinda.syahrani@student.president.ac.id,*
[2]*Faculty of Law, President University, Indonesia. E-mail: rizqyta.khoerunissa@student.president.ac.id,*
[3]*Faculty of Law, President University, Indonesia. E-mail: cindy.firdiani@student.president.ac.id,*
[4]*Faculty of Law, President University, Indonesia. E-mail: dctomasia@gmail.com,*
[5]*Faculty of Law, President University, Indonesia. E-mail: shifa.sabilah@student.president.ac.id,*
[6]*Faculty of Law, President University, Indonesia. E-mail: chelsea.goulart@student.president.ac.id,*

Article **Abstract**

Keywords:

Globalization, Information Technology, Cyber Crime, Criminal Law Enforcement Policy

Article History

Received: July 9, 2023;
Reviewed: July 12,2023;
Accepted: Aug 17,2023;
Published: Dec10, 2023

The era of globalization influences the development of technology and the internet for human life. Cybercrime can be carried out as a form of crime by involving several perpetrators in several jurisdictions of different countries, with target victims in other countries as well. This study analyzes the laws and regulations related to cybercrime in Indonesia, namely, the Criminal Code, the Telecommunications Law, the ITE Law, and the Draft Criminal Code which will become legislation in Indonesia and is based on comparative law and descriptive analysis. The research methodology uses qualitative normative legal methods with a literature study. This research also uses descriptive specifications to describe criminal law enforcement policies in eradicating information technology cri

1. INTRODUCTION

The era of globalization influences the development of technology and the internet for human life. Globalization can be interpreted as an act of process or policy-making something around the world within the scope of application. We cannot avoid technological progress in this life because technological progress will run according to scientific advances. Technology is a tool/extension of human abilities.

Technological advances produce some situations humans have never thought of before.[1]

The role of information and communication technology in the era of globalization has put in a very strategic position because it represents a world without borders, distance,space, and time. Usage influence of globalization by means of information and communication technologies have changed the lifestyle of the people, and thrive in the new order of life and promote a change in the social, cultural, economic, defense, safety, and law enforcement.[2]

Developments in information technology should be rapidly anticipated with the laws that govern them, as the negative impact should be anticipated and addressed by international law relating to the utilization of information technology crime law. Otherterms include information technology law (law of information technology), the law ofcyberspace (virtual world law), and the Cyber Law.[3]

Information technology play an important role, both in the present and in the future. Information technology is believed to bring great benefit and interest for the countriesin the world. At least there are two things that make the technology of drawing this information was considered so important spur world economic growth. First, information technology is driving the demand for information technology products itself, such as a computer, a modem, a means to build the networks, and so on.

Second, is to facilitate business transactions especially the financial business inaddition to other businesses.[4]

Technological advances have implications for the development of crime. Traditional crimes are now transformed into crimes in cyberspace (cybercrime) using the internetand other electronic tools. The internet provides opportunities for criminals in cyberspace to commit crimes more neatly, hidden, organized, and able to penetrate space and time with a broad reach. Cybercrime can be carried out as a form of crime

[1] Besse Sugiswati, Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi Di Era Informasi, *Perspektif*, Vol. 16, No. 1, 2011, page.59

[2] Sunarto, Siswanto, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari*, Rineka Cipta, Jakarta, 2009, p. 39.

[3] Explanation of Act No. 11 of 2008 on Information and Electronic Transactions, enacted on 28 April 2008, State Book No. 58.

[4] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, PT. RajaGrafindo Persada, Jakarta, 2013, p. 1-2.

by involving several perpetrators in several jurisdictions of different countries, withtarget victims in other countries as well.[5]

Cybercrime is sometimes also known as cyber sabotage and extortion. This crime is committed by disrupting, destroying, or destroying data, computer programs, or computer network systems connected to the internet. Usually, this crime is carried outby injecting a computer virus or specific computer programs so that data and computer programs cannot be used, do not run as they should, or run as desired by theperpetrator.[6]

Unlawful act in the virtual world is a phenomenon that is very worrying, given the action carding, hacking, fraud, terrorism, and the spread of destructive information has become a part of criminal activities in cyberspace. The reality that, as a stark contrast to the lack of regulations governing the use of information and communication technologies in various sectors. Therefore, to ensure legal certainty, the government is obliged to carry out the regulation of the activities associated withthe utilization of the information and communication technology.[7]

The rapid development and advancement of information and communication technologies are one of the causes of changes in human activities in various fields, directly affecting the birth of new legal acts. The government needs to develop information technologythrough the legal and regulatory infrastructure to prevent its misuse.

From the perspective of criminal law cybercrime prevention efforts can be seen from various aspects, among other aspects of the policy, criminalization (formulation of criminal offenses), aspects of criminal liability or criminal prosecution (including aspects of evidence / proof), and aspects of the jurisdiction.[8]

Rule of Law ITE has been issued by the government under Act No. 11 of 2008 on Information and Electronic Transactions (ITE Law). ITE Law is the first law that specifically regulate against cyberspace (cyber law) in Indonesia. Act ITE is a product

[5] Ismail Koto., Cyber Crime According to the ITE Law, *International Journal Reglement & Society*, Vol. 2, No. 2, 2021, page.103-110

[6] Muhammad Hatta., Efforts to Overcome Cyber Crime Actions in Indonesia, *International Journal of Psychosocial Rehabilitation*, Vol. 24, No. 3, 2020, page.1761-68

[7] Sunarto, Siswanto, Op. Cit, p. 40

[8] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*, PT Raja Grafindo Persada, Jakarta, 2007, p. 89.

of the law governing the issues in cyberspace or Internet. Within the law criminalizing arranged on several previous criminal act is not a criminal offense through some breakthroughs and expansion in terms of the principles as well as criminal sanctions. In addition to the rules of substantive criminal, in this law also regulates the procedureand evidence undergone expansion, namely the inclusion of new evidence relating to the electronic media.[9]

Anticipating cybercrime problems is not only done through the Electronic Information and Transaction Law (UU ITE) but also seeks to anticipate it in preparing the Criminal Code Bill. Based on this description, this study aims to analyze the politics of criminal law in cybercrime and how to overcome information technology crimes from cybercrime.

2. RESEARCH METHODS

The research methodology uses qualitative normative legal methods with a literature study. The literature study examines secondary data from primary and secondary legal materials. This study analyzes the laws and regulations related to cybercrime, namely the Criminal Code, the Telecommunications Law, the ITE Law, and the Criminal Code Bill, which will become legislation in Indonesia.[10] This research use descriptivespecification, which describes criminal law enforcement policy in the fight against thecrime of information technology clearly then linked with the theories of criminal justice and law enforcement practices positively linked to the research conducted.

This research explores legal norms in legislation, court decisions, and societal norms. This research also uses normative juridical methods with literature studies to analyzelaws and regulations related to cybercrime in Indonesia, descriptive specifications to describe criminal law enforcement policies in eradicating information technology crimes. The research method used is qualitative, by analyzing secondary data from primary and secondary legal materials. This study examines the Criminal Code, the Telecommunications Law, the ITE Law, and the Draft Criminal Code which will become legal regulations in Indonesia and is based on comparative law and descriptive analysis.

[9] *Ibid*, p.6.

[10] Nuria Siswi Enggarani, Penanggulangan Kejahatan Internet Di Indonesia, *Jurnal Ilmu Hukum*, Vol. 15, No. 2, 2012, page.149-168.vcxds33

3. DISCUSSION

3.1 Factors contributing to the rise of Information Technology Crimes

The rise of Information Technology (IT) crimes can be attributed to several interconnected factors:

1) Targeting people: Human error remains a primary vulnerability, as cybercriminals exploit social engineering tactics to deceive unsuspecting users into revealing sensitive information or installing malware.[11]
2) Doing their homework: Cybercriminals conduct thorough research to identify weaknesses and tailor attacks, such as spear phishing, to specific targets.[12]
3) Numbers game: The increasing number of internet users provides cybercriminals with a vast pool of potential victims, making it a lucrativeendeavor.[13]
4) Scams evolve: Cybercriminals continuously adapt their methods to circumvent improved cybersecurity measures, creating new forms of fraud and exploitation.[14]
5) Criminals sell stolen information: Illicit data is traded in underground economies, fueling further criminal activities and incentivizing cybercrime.
6) Persistence pays off: Cybercriminals exhibit patience, waiting for extendedperiods to maximize their gains and avoid detection.
7) Cheap, on-demand compute power: Advances in cloud computing enable cybercriminals to launch sophisticated attacks with minimal investment, increasing the scale and complexity of cybercrimes.

[11] Carmiel, D. (2022) *Council post: 5 trends shaping the future of Cybercrime Threat Intelligence, Forbes.* Available at: https://www.forbes.com/sites/forbestechcouncil/2022/12/19/5-trends-shaping-the-future-of-cybercrime-thre at-intelligence/?sh=58d6489830a6 (Accessed: 26 February 2024).

[12] Crane, C. (2023*) A look at 30 key cyber crime statistics [2023 data update], Hashed Out by The SSL StoreTM.* Available at: https://www.thesslstore.com/blog/cyber-crime-statistics/ (Accessed: 27 February 2024).

[13] Risks, Q.S. (2022) *8 cybercrime trends to watch out for in 2023*, *Quaker MA*. Available at: https://www.quakerma.com/8-cybercrime-trends-to-watch-out-for-in-2023/ (Accessed: 26 February 2024).

[14] Sharma, A. (no date) *Top 12 cyber crime trends to watch for in 2023*, *The National*. Available at: https://www.thenationalnews.com/business/technology/2022/12/30/top-12-cyber-crime-trends-to-watch-for- in-2023/ (Accessed: 27 February 2024).

8) Machine learning-based fraud: Criminals deploy machine learning algorithmsfor subtle and sophisticated fraud tactics that traditional anti-fraud systems struggle to detect.

9) Cross-border fraud: Global commerce and e-commerce present challenges in policing cybercrime due to jurisdictional complexities and varying regulatory standards across regions.

10) Changing e-commerce landscape: The shift towards online transactions exposes new vulnerabilities, enabling fraudsters to exploit gaps in securityprotocols and conduct fraudulent activities

11) Unclear legal jurisdiction: The absence of clear legal boundaries complicates efforts to prosecute cybercriminals engaged in cross-border operations, allowing them to operate with impunity

12) Negligence: Failure to implement adequate security protocols creates opportunities for cybercriminals to exploit vulnerabilities and launchsuccessful attacks.

13) Loss of evidence: Digital traces of criminal activity can be easily deleted or obscured, hindering investigative efforts and making it challenging to prosecute cybercrimes effectively.[15]

3.2 Impact of Information Technology Crime on Individuals and Society in Individuals:

1) Financial loss: One of the most common impacts of cybercrime on individualsis financial loss. Cybercriminals often use various methods such as phishing, hacking and malware to gain access to a person's financial information, such as credit card numbers, bank account details and passwords. This can result inthe loss of money through unauthorized transactions, which is difficult to recover.
2) Identity theft: Identity theft is another significant consequence of cybercrimefor individuals. Cybercriminals can use stolen personal information such as social security numbers, driver's license numbers, and dates of birth to open

[15] Platts, T. (2023) *Cybercrime trends in 2023 and beyond, Nexstor.* Available at: https://nexstor.com/emerging-trends-in-cyber-crime/ (Accessed: 27 February 2024).

new accounts, take out loans, and commit other types of fraud in a person's name.

3) Emotional trauma: In addition to financial loss and identity theft, cybercrimecan cause emotional trauma. Victims of cybercrime often feel violated and vulnerable, giving rise to fear and anxiety. This can have a long-term impact on a person's mental health, especially if they feel isolated and unable to seekhelp.
4) Loss of reputation: Lastly, cybercrime can damage a person's reputation. Cybercriminals can use stolen information to post embarrassing or damaging content online, causing a loss of credibility and trust. The impact of reputational damage can be devastating in a professional environment, leadingto job loss or difficulty finding employment.

In society:

1) Economic impact: Cybercrime can have a significant impact on the economy.This can result in financial losses for individuals, businesses and the government. The costs of repairing system damage, recovering lost data, and preventing future attacks can be enormous.
2) National security concerns: Cybercrime can pose a serious threat to national security. Attacks on government and military networks can compromise sensitive information and disrupt operations. Cybercriminals can also use technology to conduct espionage, steal state secrets, and disrupt critical infrastructure, such as power grids and transportation systems. Additionally, cybercrime can be used for political and ideological purposes, causing socialand political unrest.
3) Impact on health services and public safety: Cybercrime can have a significantimpact on health services and public safety. Attacks on healthcare systems cancompromise sensitive patient data and disrupt medical services, which can have life-threatening consequences.
4) Increased cyberbullying and harassment: Cybercrime can lead to an increase in cyberbullying and harassment, as cybercriminals use technology to target individuals and groups, spreading harmful content and harassing messages, causing emotional and psychological harm, reputational damage, problems

mental health such as depression and anxiety, as well as spreading misinformation.

5) Social media manipulation: Social media manipulation is a form of cybercrimethat involves the use of social media platforms to influence, deceive, or manipulate individuals or groups for political, financial, or personal gain. This can take many forms, including spreading false information, creating fake profiles or personas, and using bots or automated accounts to amplify messages. The impact of social media manipulation on society can be enormous, as it can undermine the integrity of democratic processes, spread extremist ideologies, and erode public trust in institutions and information sources. Therefore knowing prevention strategies is important.[16]

3.3 Challenges faced by Law Enforcement agencies in addressing Information Technology Crime

One of the main challenges facing law enforcement agencies in the investigation of online exploitation and obscenity, and cyber stalking is the fact that these activities occur in an environment that is difficult to effectively and accurately monitor in terms of the actual activities of individual online users. The technological barriers associated with monitoring online activity include the hardware and software protective systems that people use to prevent unauthorized access to personal data through the Internet.

For example, encryption of online transmissions prevents monitoring by lawenforcement agencies.[17]

There have 5 key challenges for law enforcement agencies in addressing Information Technology Crime;

1) Loss of Data

Due to legislative changes such as the GDPR, law enforcement may be denied access to data or may only be able to access very limited data as part of a criminal investigation. Increasing technological development and internet use

[16] Welance (2023) *Impact of cybercrime on individuals, businesses, and society., LinkedIn.* Available at: https://www.linkedin.com/pulse/impact-cybercrime-individuals-businesses-society-join-welance/ (Accessed: 25 February 2024).

[17] Elizabeth Nelson *(2021) Law Enforcement Challenges in Online Environments.* Available at: https://dovney.com/law-enforcement-challenges-in-online-environments. (Accessed: 26 February 2024).

also presents a challenge for law enforcement, resulting in extremely large amounts of data where it is difficult to distinguish a specific user.

Encryption is another tool used by criminals to stop incriminating data from getting into the hands of law enforcement, whilst the use of cryptocurrencies such as Bitcoin allows criminals to deal in the proceeds of crime with a relative level of anonymity. Lack of data required by law enforcement has a significant detrimental impact on their work, often resulting in investigations being delayed or even discontinued.[18]

2) Loss of Location

The use of encryption, cryptocurrencies and other technologies such as the dark web or cloud storage may result in the loss of data, they also present significant challenges for law enforcement in establishing the physical location of perpetrators, criminal infrastructure or electronic evidence. This raises complex jurisdictional considerations and makes it difficult to determinewho is responsible for conducting investigations.[19]

3) Lack of Cooperation with the Private sector to address Cybercrime

Law enforcement agencies and Private sector organizations are rarely on the same page also leads to an Inefficient and slower response to the issue, whichcan put the public at risk

4) The Complexities of International Cybercrime

The lack of a common regulatory framework makes it difficult for countries to address the issue. Because of the different laws and legislation in each country,there is a lack of standardization in the field which leads to a slower response. A lack of data sharing also makes it a challenge because of a lack of information sharing between countries.[20]

[18] Miralis, D. *(2020) The 5 key challenges for law enforcement in fighting cybercrime, Lexology*. Available at: https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dc-cd91826f05d4 (Accessed: 26 February 2024).

[19] *The 5 key challenges for law enforcement in fighting cybercrime* (2021) NGM Lawyers. Available at: https://ngm.com.au/cybercrime-5-key-challenges/ (Accessed: 27 February 2024).

[20] *International cooperation against Cybercrime - cybercrime - www.coe.int* (no date) *Cybercrime*. Available at: https://www.coe.int/en/web/cybercrime/international-cooperation (Accessed: 26 February 2024).

5) Lack of public and Legal awareness

The lack of public and legal awareness also plays a role. Since cyber crime is a growing issue, the lack of public awareness can make it easier for criminals to target people. The lack of information about the legal system and its laws can also lead to a slow response to dealing with cyber crime. This lack of public awareness can also lead to misconceptions about the laws and lead to people not knowing what is legal and what is illegal in the online world. This can leadto people not being careful online which makes them easier victims for cyber criminals. So the lack of public and legal awareness can also be a factor that can slow down the process of dealing with and addressing cyber crime cases.[21]

3.4 Role of Law Enforcement agencies in combating Information Technology Crime

Law enforcement agencies play a crucial role in combating information technologycrime, such as cybercrime. They are at the forefront of responding to cybercrimes, which include activities like identity theft, financial fraud, child pornography, and more. Here are some key points regarding the role of law enforcement agencies in combating information technology crime based on the provided sources:[22]

1) Capacity Building: Law enforcement agencies need to enhance their cybercrime capacity and capability through additional training, improved communication, collaboration, and updated cybercrime models.
2) Training and Resources: Agencies require up-to-date technological tools and equipment for electronic crime investigations. This includes essential cybertools, software, hardware, intrusion detection tools, decryption technology, and exposure to higher-end computer technology.
3) Collaboration: Collaboration with the private sector is critical in combating cybercrime. Law enforcement agencies work with private companies to develop trusted relationships, share equipment for examining electronic evidence, and encourage reporting of electronic crime.

[21] Author links open overlay panelDr. Vasileios Karagiannopoulos a *et al.* (2021) *Cybercrime awareness and victimization in individuals over 60 years: A portsmouth case study*, *Computer Law & Security Review*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364921000881 (Accessed: 27 February 2024).[22] *Assessing law enforcement's cybercrime capacity and capability* (2022) *FBI*. Available at: https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability- (Accessed: 26 February 2024).

4) Prevention and Investigation: Local law enforcement agencies are involved in preventing and investigating cyber crimes by actively looking for illegal cyber activity or offenders, participating in prevention initiatives, providing specialized training to personnel in computer crime units, and using regional or statewide programs for training
5) Partnership with Industry: Partnering with law enforcement can help track incidents, thwart attacks, pursue prosecution, deter criminals from committing crimes, and dismantle criminal infrastructure used in cybercrimes.

3.5 Effectiveness of current Criminal Law enforcement Policy Efforts

Current criminal law enforcement policy efforts are effective in preventing and combating information technology crime for some but not as effective for others due to various factors, including resource constraints. Efforts by agencies like the New Jersey State Police High Tech Crime Bureau, which consists of specialized units like the Cyber Crimes Unit and the Regional Computer Forensic Laboratory, aim to address cybercrimes effectively. The use of advanced technology in the criminal justice field has transformed the landscape, offering both opportunities and challenges. Technologies like artificial intelligence, facial recognition, biometrics, wearables, and high-end management software have enhanced law enforcement capabilities. These advancements have improved investigations, policing accuracy, forensic analysis, surveillance, and monitoring in criminal justice operations.[23]

One major issue contributing to the ineffectiveness of these policies is the lack of resources and funding allocated to combating information technology crime. Without adequate support, law enforcement agencies are unable to effectively investigate andprosecute cybercriminals. In order to improve the effectiveness of current criminal law enforcement policies, there needs to be a greater investment in resources and funding dedicated to combating information technology crime. Additionally, collaboration between law enforcement agencies, cybersecurity experts, and private sector organizations is essential in addressing this evolving threat landscape. Only

[23] *Assessing law enforcement’s cybercrime capacity and capability* (2022a) *FBI.* Available at: https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability- (Accessed: 27 February 2024).

through a comprehensive approach can we hope to effectively prevent and combat information technology crime.[24]

4. CONCLUSION

The rapid development of information and communication technology in the era of globalization has brought tremendous benefits to countries worldwide, driving economic growth and facilitating business transactions. However, this progress has also led to the proliferation of information technology crimes, presenting significant challenges for law enforcement agencies. Despite efforts to regulate cyber activities through laws like the Electronic Information and Transaction Law (UU ITE) and the Draft Criminal Code, challenges such as loss of data, encryption, jurisdictional complexities, and lack of cooperation persist. To enhance the effectiveness of criminal law enforcement policies, there is a need for capacity building, collaboration with the private sector, prevention initiatives, and increased resources allocation. Only through a comprehensive and collaborative approach can we effectively combat information technology crimes and safeguard individuals and society in the digital age.

REFERENCES

Book

Budi Suhariyanto, Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya, (PT. RajaGrafindo Persada, Jakarta, 2013) [1-2] https://perpustakaan.bldk.mahkamahagung.go.id/index.php?p=show_detail&id=6951&keywords=

Barda Nawawi Arief, Tindak Pidana Mayantara: *Perkembangan Kajian Cyber Crime di Indonesia*, (PT Raja Grafindo Persada, Jakarta, 2007) [89]
https://inlislite.uin-suska.ac.id/opac/detail-opac?id=18928

Barda Nawawi Arief, 2006, Mayantara's *Crime Development of Cybercrime Studies in Indonesia,* Raja Grafindo Persada, Jakarta.

[24] (No date) *The role of local law enforcement agencies in preventing ...* Available at: https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/ the role of local law enforcement agenciesin preventing and investigating cybercrime 2014.pdf (Accessed: 27 February 2024).

Regulation

Explanation of Act No. 11 of 2008 on Information and Electronic Transactions, enacted on 28 April 2008, State Book. https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008

Journal/Article

Besse Sugiswati, Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi Di Era Informasi, (vol. 6, 2011, Perspektif, Fakultas Hukum Wijaya Kusuma Surabaya) [59] https://ejournal.uwks.ac.id/myfiles/201207530921134643/6.pdf

Sunarto, Siswanto, Hukum Informasi dan Transaksi Elektronik *(Studi Kasus Prita Mulyasari).* (Rineka Cipta, Jakarta, 2009) [39] http://opac.lib.unlam.ac.id/id/opac/detail.php?q1=340&q2=Sun&q3=H&q4=-

Ismail Koto, Cyber Crime According to the ITE Law: *International Journal Reglement & Society*, (Vol. 2, 2021) [103-110]
https://jurnal.bundamediagrup.co.id/index.php/ijrs/article/download/124/112

Muhammad Hatta, Efforts to Overcome Cyber Crime Actions in Indonesia: *International Journal of Psychosocial Rehabilitation*, (Vol. 24, 2020) [1761-68] https://repository.unimal.ac.id/5339/1/04.%20Jurnal%20Psychosocial%202.pdf

Sunarto, Siswanto, Hukum Informasi dan Transaksi Elektronik *(Studi Kasus Prita Mulyasari).* (Rineka Cipta, Jakarta, 2009) [40] http://opac.lib.unlam.ac.id/id/opac/detail.php?q1=340&q2=Sun&q3=H&q4=-

Nuria Siswi Enggarani, Penanggulangan Kejahatan Internet Di Indonesia: *Jurnal Ilmu Hukum*, (Vol. 15, 2012, Universitas Muhammadiyah Surakarta) [149-168] https://publikasiilmiah.ums.ac.id/bitstream/handle/11617/4010/4.pdf?sequence=1&isAllowed=y

Ariffin, Khairul Akram Zainol, and Faris Hanif Ahmad, ‘Indicators for Maturity and Readiness for Digital Forensic Investigation in Era of Industrial Revolution 4.0’, Computers and Security, 105 (2021), 102237
https://doi.org/10.1016/j.cose.2021.102237

Gruber, Jan, Lena L. Voigt, Zinaida Benenson, and Felix C. Freiling, ‘Foundations of Cybercriminalistics: From General Process Models to Case-Specific Concretizations in Cybercrime Investigations’, *Forensic Science International: Digital Investigation*, 43 (2022), 301438 https://doi.org/10.1016/j.fsidi.2022.301438

Ćmiel, Sylwia, ‘Cyberbullying Legislation in Poland and Selected EU Countries’, *Procedia - Social and Behavioral Sciences*, 109 (2014), 29–34 https://doi.org/10.1016/j.sbspro.2013.12.416

Website

Carmiel, D. (2022) *Council post: 5 trends shaping the future of Cybercrime Threat Intelligence, Forbes.* Available at: https://www.forbes.com/sites/forbestechcouncil/2022/12/19/5-trends-shaping-the-future-of-cybercrime-threat-intelligence/?sh=58d6489830a6 (Accessed: 26 February 2024).

Crane, C. (2023*) A look at 30 key cyber crime statistics [2023 data update], Hashed Out by The SSL StoreTM.* Available at: https://www.thesslstore.com/blog/cyber-crime-statistics/ (Accessed: 27 February 2024).

Sharma, A. (no date) *Top 12 cyber crime trends to watch for in 2023, The National.* Available at: https://www.thenationalnews.com/business/technology/2022/12/30/top-12-cyber-crime-trends-to-watch-for-in-2023/ (Accessed: 27 February 2024).

Platts, T. (2023) *Cybercrime trends in 2023 and beyond, Nexstor.* Available at: https://nexstor.com/emerging-trends-in-cyber-crime/ (Accessed: 27 February 2024).

Welance (2023) *Impact of cybercrime on individuals, businesses, and society., LinkedIn.* Available at: https://www.linkedin.com/pulse/impact-cybercrime-individuals-businesses-society-join-welance/ (Accessed: 25 February 2024).

Elizabeth Nelson *(2021) Law Enforcement Challenges in Online Environments.* Available at: https://dovney.com/law-enforcement-challenges-in-online-environments. (Accessed: 26 February 2024).

Miralis, D. *(2020) The 5 key challenges for law enforcement in fighting cybercrime, Lexology.* Available at: https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dc-cd91826f05d4 (Accessed: 26 February 2024).
International cooperation against Cybercrime - cybercrime - www.coe.int (no date) *Cybercrime.* Available at: https://www.coe.int/en/web/cybercrime/international-cooperation (Accessed: 26 February 2024).

Author links open overlay panelDr. Vasileios Karagiannopoulos a *et al.* (2021) *Cybercrime awareness and victimization in individuals over 60 years: A portsmouth case study, Computer Law & Security Review.* Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364921000881 (Accessed: 27 February 2024).

Assessing law enforcement's cybercrime capacity and capability (2022) *FBI.* Available at: https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability- (Accessed: 26 February 2024).

(No date) *The role of local law enforcement agencies in preventing ...* Available at: https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/ the role of local law enforcement agencies in preventing and investigating cybercrime 2014.pdf (Accessed: 27 February 2024).

Koto, Ismail., *Cyber Crime According to the ITE Law,* International Journal

Reglement & Society, (Vol. 2, 2021).

Levi, Michael and Matthew Leighton Williams., *Multi-Agency Partnerships In Cybercrime Reduction Mapping The UK Information Assurance Network Cooperation Space, Information Management &Computer Security,* (Vol. 21, No. 5, 2013).

Enggarani, Nuria Siswi., *Penanggulangan Kejahatan Internet Di Indonesia*,
Jurnal Ilmu Hukum, (Vol. 15, 2012).