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

Ai in Cybercrime Legal Responses to the use of Artificial Intelligence in Ransomware and Phishing Attacks

Arunachala Muthulingam[1], Vidhya Lakshmi V[2]

[1,2]Student Sastra Deemed University

ABSTRACT

The fast development of Artificial Intelligence has caused the transition of standards and techniques in various industries, but this has also brought in new challenges, especially in the area of cybercrime. It is used mostly to create highly powerful ransomware and phishing attacks, thus making them very dangerous for personal security, and especially for the security of the nation and an organization. Ransomware and phishing attacks usually prey on manual skills to defraud familiar individuals. Yet, using AI, criminals were able to create more efficient attacks that are much harder to detect. Its algorithms can design personalized phishing emails by reviewing immense data sets in a highly efficient manner, which directly results in a convincing email. This would then make the email look convincing and help the attacker have the highest possibility of success. The laws that are used to prevent such crimes are not as effective as they can be when it comes to the newer AI-related nuances that make direct liability determination much trickier when the AI system is acting on its own. The cross-border activity of hackers is usually the result of differences in laws and technology enforcement capacity. Although there is a difference of opinion amongst various nations all should come together when it is the question of national security. This paper analyses the legal responses and liability regarding the growing use of AI in these cybercrimes, with focus on the existing legal frameworks and the challenges and developments to be addressed.

Keywords: Artificial Intelligence, Ransomware, Phishing, Legal Framework, Cybercrimes

Background

Ransomware is a category of harmful software that encrypts files to prevent access to a computer system or data. The virus then demands payment in cryptocurrency to unlock the contents. Unless the ransom is paid, the attacker tends to threaten to erase or share the data of the victim. Attacks by ransomware targeting individuals as well as organizations have become more advanced since they became targeted and faster, with the use of artificial intelligence (AI). Phishing refers to an attack in which the perpetrators assume the identities of respectable organizations in a ploy to hoodwink victims into providing private information, credit card numbers, or other personal information. Most phishing attacks happen through instant chat, email, or rogue websites where vulnerable victims download malware or click on unsafe links. Attackers are now able to use AI and make more convincing emails and which are difficult to detect it. The term "phishing" gained popularity around 2003. Social engineering tactics were employed by attackers to send phony emails purporting to be from reputable companies like PayPal or eBay. These attacks were aimed at soliciting personal information by exploiting people's trust and gullibility. Between

2004 and 2006, "spear-phishing" became quite widespread when phishing attacks started to become more sophisticated. Spear-phishing is what is referred to as highly targeted attacks targeted at specific people or organizations. Attackers would obtain victims' personal information to give the phishing attempts more legitimacy. The AIDS Trojan attack was one of the first ransomware attacks which was created by Dr. Joseph Popp and distributed to 20,000 attendees of an AIDS conference. Eddy Willems, a Belgian IT expert received an infected diskette that encrypted all of his files and demanded ransom money, and only after the attack's massive scale, his decryption method went around the world, raising Willems' career in cyber defense. Ransomware schemes, although very profitable, did not proliferate because the criminals encountered many difficulties while collecting the payments through traditional methods. However, the emergence of Bitcoin in 2013 brought in a new hero, as it pushed the crypto-text ransomware to the back seat. Instead, this was the starting point of a new destructive level of ransomware attacks led by CryptoLocker.

Currently, phishing attacks have been perpetually evolving and are increasingly making use of automation and AI. The hackers started using it to create emails, chats, and even films that look so authentic they almost simulate real people or organizations. In this phase, the trend is also gaining as for Business Email Compromise (BEC) scams, wherein robbers pose as executives or workers to steal money from businesses. Artificial intelligence is developing ransomware and phishing attacks to seem more sophisticated, automated, and customized. AI is being used by cybercrooks to increase the scope and impact of operations for phishing attacks. Artificial intelligence makes it possible to create convincingly realistic phishing emails targeted at specific users through analyzing massive databases of personal information, their social media activity, and internet behavior. India has seen a 53 percent increase in ransomware incidents in 2022. phishing is the most common entry point for ransomware attacks, accounting for 41 percent of these cases. AI will change ransomware and phishing attacks in the future, making them more effective. Such an AI arms race would eventually spring up, with offensive and defensive systems competing with each other, but may also result in ever more complex and upkeep-intensive cybersecurity ecosystems in the future.

LITRATURE REVIEW

The rapid evolution of artificial intelligence (AI) has significantly impacted the field of cybersecurity, presenting both new opportunities and challenges. The study by Chakraborty Et Al(2023) highlights how AI has transformed cybersecurity, enhanced protective measures, and introduced new vulnerabilities. They emphasize that traditional threats, such as malware and phishing, have evolved into more complex AI-powered attacks, necessitating the adoption of AI-based defenses like threat detection and behavioral analytics to combat these emerging risks. They suggest that the future of AI in cybersecurity lies in predictive analytics and autonomous systems, underscoring the importance of ethical AI development.

The study by Siddiqui and Et Al(2018) elaborates on the necessity for innovative solutions to address the pervasive threat of cybercrime. Their review reveals that conventional security measures often fall short against sophisticated attacks, which has led to the emergence of AI as a promising tool for cybercrime detection and prevention. They explore various AI techniques that have been effective in identifying and mitigating cyber threats, while also highlighting areas for future research to enhance AI’s capabilities in safeguarding IT infrastructures.

Tetaly and Kulkarni (2022) examine the dual nature of AI in cybersecurity, recognizing its potential to serve both as a solution and a threat. They point out that the growing reliance on data heightens the stakes

in cybersecurity, as traditional measures become increasingly inadequate. Their analysis calls for robust safeguards in the implementation of AI-driven security solutions to prevent exploitation by adversaries. They discuss the various applications of AI, acknowledging the potential for malicious use alongside its benefits, and propose strategies to mitigate the vulnerabilities of AI systems against hacking and data theft. While these above-mentioned studies focus on the capabilities of AI in enhancing cybersecurity, Ghazi-Tehrani and Pontell(2022) take a different approach by analyzing the evolving nature of phishing attacks. They explore technological measures to combat these threats but leave a significant gap regarding the legal frameworks for addressing phishing and ransomware incidents. This highlights a critical need for research into harmonized legal frameworks that can regulate and protect individuals and organizations from cybercrime effectively.

The study by Fabian Teichmann(2023) investigates the potential of generative AI to facilitate ransomware attacks, demonstrating that individuals with varying levels of IT expertise can leverage AI-powered chatbots to plan and execute sophisticated attacks. The author's analysis highlights the risks posed by the widespread availability of generative AI, suggesting that it could increase the frequency and effectiveness of ransomware incidents. By combining criminological techniques with an analysis of AI's potential criminal applications, the study provides valuable insights for future research in cybersecurity, IT law, and criminology.

The development of AI has significantly impacted cybersecurity, providing tools for both offensive and defensive purposes. Cybercriminals have leveraged AI to automate phishing, generate malware, and engage in social engineering, while AI-driven defenses can enhance threat detection, incident response, and security patch management. Organizations must invest in AI-powered security solutions to effectively address the evolving threat landscape, educate their employees, and stay informed about emerging trends and best practices. Overall, the literature underscores a consensus on integrating AI into cybersecurity strategies while simultaneously addressing the ethical and legal challenges it poses. The gap in legislative discourse indicates a pressing need for comprehensive frameworks to safeguard rights and assets in the face of increasingly sophisticated cyber threats.

RESEARCH PROBLEM

Indian Legal and regulatory frameworks governing AI in ransomware and phishing attacks are ill-equipped and provide wide flexibility that is possibly being misused and hence need legislative amendments or a sui generis law to make them more concise and improve transparency and accountability.

RESEARCH OBJECTIVE

This research aims to critically assess India's legal and regulatory frameworks governing artificial intelligence (AI) in ransomware and phishing attacks. The objective is to enhance transparency, accountability, and liability in AI-driven cybercrime, ensuring better protection for various sectors in India against rising AI-enabled threats.

RESEARCH QUESTION

1. Whether insufficient legal responses and the current legal framework be effectively modified to address AI-driven ransomware and phishing challenges?
2. Whether the responsibility for AI-generated ransomware and phishing attacks should lie with developers, operators, and organizations deploying the AI, or be distributed among them?

SCOPE AND LIMITATIONS

The research will be guided by the legal and regulatory framework of India on cybercrime and how such a framework applies to AI-driven ransomware and phishing attacks. The comparative analysis of legal standards and frameworks controlling AI in cybercrime especially as practiced in the EU are what the research will involve. It will focus on the proposal for amendments of existing Indian laws through legislation recommend the development of a sui generis legal framework for AI-enabled cybercrimes and explore legal theories of accountability in AI-generated cyberattacks. The AI application research here is mainly on ransomware and phishing attacks, though may not focus on all kinds of AI-driven cybercrimes or other types of cyber threats whose identification is through AI.

Although the research will be comparative in legal analysis, its scope will be limited to only a few important international jurisdictions and therefore not cover all global legal systems that regulate AI and cybercrime. AI technologies as well as cybercrime techniques change very rapidly; research findings and recommendations may have to be updated constantly as new developments arise.

CHAPTERS OF THE PAPER

Potential consequences of inadequate legal responses to Al-enabled cybercrime

Legal frameworks and statutes and their responses play a vital role in structuring and regulating crimes. Inadequacy in legal frameworks can lead to numerous grave effects concerning cybercrime enabled through AI, which affects not only corporations but also individuals and national security. Where legal measures are weak or unavailable, cyber thieves will exploit AI technologies to their best advantage. More opportunities will emerge to amplify AI-based ransomware, phishing, and other cybercrimes. Additionally, AI can be exploited more aggressively to automate and perfect criminal activity if the legal effect is insignificant or not enforced.Financial Impacts are a huge hit on organizations and individuals involved, the economic impact can be greatly felt. One of the significant reasons, AI-driven attacks can financially impact on a massive scale is the ransom, loss of confidential information, and the often-heavy costs required to recover and secure compromised systems. Businesses may also suffer a reputational loss that will further eat into their revenue.

- **Challenges of International Jurisdiction**: Most cross-border AI-powered cybercrimes pose more challenges to the enforcing agencies because they raise issues that go beyond the international border. Such cross-border crimes are also challenging to prosecute due to weak and inadequate legal structures of the countries concerned. Moreover, there is no international uniform regulation of AI-powered cybercrime.
- **Data Privacy Violation**: AI-attack on private data could result in severe privacy violations wherein people might easily be exposed to risks like identity theft and fraud. Violations not only harm the victim but also arouse immense disbelief in the capability of businesses as well as governments at all levels to protect sensitive information.
- **Technological Innovation Stagnation**: Companies may refrain from investing in artificial intelligence and other digital innovations due to the fear of vast AI cyberattacks or legal liability during AI misuse. Such restraint would lead to a decline in technological growth as companies would be more risk-averse and avoid new technologies without sound legal protection.
- **National Security Vulnerabilities**: The absence of sufficient legal measures presents a vulnerability to critical infrastructure—e.g., the energy systems, health care facilities, and transportation networks—

since AI-aided cyberattacks can shut off crucial services and incite mass pandemonium and even people's lives in danger.

- **Ambiguity in Liability and Accountability:** The existing law structures under which law enforcement agencies try to curb cybercrime often lack sufficient engagement with the peculiar challenges posed by AI-related cybercrime. If these legal structures are not reformed, it will be practically impossible to identify liability in the case of an AI system behind a cyber-attack. This ambiguity introduces legal loops that the cyber-criminal can exploit and makes accountability almost difficult to pursue against such offenders.

An Overview of European Union AI Laws and what can be taken from it to India

This leaves room for adopting existing legal frameworks to handle AI-generated ransomware and phishing attacks, taking a multi-layered approach along lines of updating the existing laws, international cooperation, and accountability. Here are key strategies for adapting legal frameworks: India and the European Union (EU) are making different progress in regulating artificial intelligence, not only because of differences in their technology environment, agendas, and legal framework but also in the strategic approach they have towards the regulation of AI. In comparison, this will thus be an important lesson for India to consider the fundamental contrasts and similarities to be kept in mind while developing its AI regulatory laws.

AI Act (Drafted in 2021): One of the most comprehensive legislative regimes especially for AI technologies is the proposed AI Act of the EU. It is set on a risk-based approach with four classes by danger levels for AI systems:

Privacy, Security with Unacceptable Risk: AI systems that seriously infringe on fundamental rights which are prescribed (e.g. right to life includes right to privacy also).

High Risk: AI applications that fall within critical domains like healthcare, education, or law enforcement are subject to very strict standards.

Low Risk: AI applications with minimal risks like chatbots still need to meet transparency standards.

Minimal Risk: Low to no risk AI applications like spam filters hold very minor responsibilities.

The AI Act primarily focuses on the responsibility and transparency aspects of accountability, making high-risk AI systems produce explainable results. The AI Act makes the users, developers, and providers accountable and responsible to ensure that AI is applied with democratic principles and human rights.The GDPR has already begun some level of regulation of AI systems that handle personal data. The GDPR legally imposes obligations upon AI systems to protect the privacy of users and to empower them to have control over their data and impose severe consequences in case of non-compliance.

AI Ethics Guidelines: European Union has taken an approach to add to the legal framework by providing ethics guidelines in AI that concentrate on developing trustworthy AI and call forth values such as justice, accountability, and non-discrimination.

Key Comparisons:

India vs. EU on AI Regulation:

The regulatory framework in the EU has categorized AI systems into a comprehensive, well-structured, and risk-based approach. Several systems fall into different categories of risks. High-risk systems have more binding rules with it, focused on ethics, accountability, and transparency. India is less strict on the laws and more eager to push AI ahead for progress and development. India's legal system is still developing, with an emphasis mostly on the monetary benefits of AI.

Data protection-The EU's GDPR possesses a strong framework of legislation for AI, especially concerning personal data. The strenuous limits on data privacy under the GDPR apply to AI systems operating in the EU and infractions will attract penalties. This Data Protection Bill from India is going to be highly significant in shaping the use of AI to process personal data.India's structure, though well accepted, has been most stringently criticized for being too lenient during its enforcement period.

Accountability: The EU has enacted the AI Liability Directive so that victims receive compensation for damages they inflict through their AI. This makes it less complicated to get a customer to file a lawsuit because of this. India does not have a defined framework for AI system responsibility and, therefore, it is difficult to establish accountability towards harm caused by AI activities themselves, whether they were merely powered by or implemented by AI developers or operators.

India's takeaway from EU's AI law:

Here, the AI framework by the EU offers opportunities for India to classify high-risk versus low-risk AI systems. Such classification would allow India to regulate AI more strictly in such sensitive fields as health care and finance, while remaining lenient in other areas. India may take over the EU responsibility of liability in creating liability for AI system developers and deployers. This can be achieved by the preparation of an exact AI liability law that holds creators responsible for the damage generated by their AI systems just like the EU's AI Liability Directive. India can benefit from AI development focusing on accountability, fairness, and transparency-that are the basics of the EU recommendations. The most significant aspect for India has to focus on the development of more effective forming procedures for enforcement and stricter punishments related to data protection violations so that personal data in this context becomes safe in AI systems.

The extent of liability on key players:

The question of who is to be blamed for ransomware and phishing attacks launched by AI because AI grants autonomous decision-making capabilities, to which malicious entities can misuse, is a very complex issue. Apart from the developers of such ransomware and phishing attacks, there are still other parties who can potentially become liable, yet the current legal frameworks often leave the liability status ambiguous. Some significant liability factors include the following:

The Creator of the AI System:

If its designers so carelessly created and exposed it to misuse in cyber attacks, then there is a basis for liability against them. When an AI system was created to execute dangerous tasks but did not follow security instructions, then an argument may be presented that the creator of the AI bears partial liability if the protection against misuse by hostile parties is insufficient. However, this begs the following question: just how much is the developer actually paying for it? It indeed becomes much harder to hold a well-intentioned AI system developer liable if a system was later used for malicious purposes by cybercriminals, especially if an exploitation could not be reasonably contemplated.

The User or Operator of the AI System:

Under present cybercrime laws, it would be the person or organization conducting ransomware or phishing attacks with AI that would normally hold liability. It is the one who intentionally employs an AI tool to create malicious code or manipulates AI for conducting cyberattacks who should mainly be given legal liability. Because the operator intends to cause injury or to cheat, this tactic is very much within the bounds of current legal rules.Since the intent of the operator is clearly to cause injury or commit fraud, this strategy is consistent with current legal rules. The trouble begins when the AI function operates partially independently, and the human operator does not control all the decisions.

The AI-generated attacks by itself (Autonomous AI Liability):

It is even doubtful whether the AI system should be liable at all. However, in that case, the AI system cannot be "punished" or considered liable in a very conventional legal sense because this is a non-human entity. Some legal scholars propose new legal positions for artificial intelligence (AI) entities that can be made liable under specific conditions.When an AI autonomously generates attacks, it can be made liable along with the person who is benefited by those attacks. The AI system should be barred or inserted with restriction software to prohibit it to involved in more generations of ransomware and phishing attacks.

Organization Using the AI System:

An organization will be liable if it uses an AI technology that, inadvertently or intentionally, leads to phishing or ransomware attacks. This becomes truer if the firm exploits or puts in place AI systems with inadequate security measures or due diligence. Businesses employing AI-based marketing or data analytical tools that may be used to start phishing attacks, among others, risk legal sanctions if they fail to adhere to strict cybersecurity standards. Besides, if a company has a legitimate use for AI and its system is therefore breached and used to commit crimes, the company could be liable if proper cybersecurity measures were not put in place.

Cybercriminals using AI Tools: In other cases, most direct responsibility is left to cybercriminals using AI tools to craft phishing or ransomware attacks. As well, it is also hard to trace or prosecute them since they usually operate in secret and from various international boundaries. It is not easy to prosecute cyber criminals due to a jurisdiction issue, and cross-boundary legal frameworks for cybercrime enforcement are still under development.

Shared or Collective Responsibility: There shall be moments when the developer, operator, and user share the responsibility on account of the multiplicity of parties involved in the development, deployment, and usage of AI. For instance, if a business organization uses a third-party-developed AI system and neither the parties have taken careful considerations to ensure that the system is secure, then both parties would be liable for whatever damage that occurs.

Possible doctrines attributable to AI attacks:

1. Vicarious Liability:

Vicarious liability is liability based on wrongful acts of a party imputed to another because of some particular relationship subsisting between them, for example, employer-employee or principal-agent. In other words, the person liable here is, more often than not, the employer or principal for the acts of the person under his control employee or though he hasn't directly committed the act or approved it. In such a scenario, might the company be held liable for what the AI does that it was not intended to or foreseen by the company when an AI system employed by a company autonomously launches a phishing or ransomware attack? The conditions of autonomy for AI systems bear little resemblance to those used when discussing employees. AI systems have no intent or consciousness. They work purely based on algorithms and data. It's impossible to lend any sort of agency or authority the way it traditionally applies.

Employers and Employees: Vicarious liability operates on the relationship between the employer and employee, and AI lacks the human elements typified in that relationship. The courts should, therefore, look into whether the AI system qualifies to be described as an "agent" or "employee" under the law or whether liability falls to the creators or users of the system. Foreseeability: An important factor in the facts of respondeat superior is whether the tortious act was within the ambit of employment or agency. Again,

for AI, it is less than clear if autonomous decisions made by AI can be considered foreseeable actions within the purview of the responsibility of the employer.

2. Contributory Negligence:

One of the defenses to an action for damages is contributory negligence, which can even bar a plaintiff's right to recover damages when they themselves were partly to blame for their resulting harm. In this area of the legal doctrine, if the party injured, the plaintiff, was at least partially negligent and their negligence contributed to the actual injury suffered, then they may not be able to receive compensation or the judgment award will severely be reduced. Key Ingredients of Contributory Negligence is that a Plaintiff's Own Negligence. The plaintiff must have acted in a manner which has breached a duty of care to themselves. For example, it may be that they do not follow the proper safety procedures or that they act in a reckless manner or fail to take reasonable care to avoid harming. The comparative fault of the claimant shall have contributed in the causation of the harm or injury he has suffered. Barely a minimal percentage will disqualify or limit his right to recover damages. It means that if the company or individual failed to exercise reasonable care, by not patching up the vulnerabilities in its software, then they can be held contributorily negligent in case of an AI-powered cyberattack. For example, in a healthcare system attacked by AI-generated ransomware where such a healthcare system fails to have appropriate security, the liability for both the AI creator and the one deploying AI will be diminished upon contributory negligence. Failure to Mitigate Damages is the other element included in contributory negligence. When the victim of AI phishing fails to act as speedily as possible to salvage the damage, this doctrine cuts down the claimant's damages.

3. Strict Liability:

Strict liability is a principle of law. Here, liability is attached on one, either for damage or harm that has resulted from his acts or products with no fault or showing intent to bring about such harm Under strict liability, the element of fault or negligence is not required; it simply arises on account of the dangerous character of the activity or product involved. If an AI system, when considered intrinsically dangerous-that is, a system developed for cybersecurity but then adapted for attacks, strict liability can be triggered. In this case, the action taken by the cyberattack from this AI system can be attributed to the developers or users without regard to intent. Strict liability in product liability cases is not unheard of today; an artificial intelligence system could be subjected to the same rule. The courts would then consider whether a product with artificial intelligence had proper safeguards so that it wouldn't be used in harmful ways. The creators of that artificial intelligence could be strictly liable for damage caused by autonomous actions, such as phishing or ransomware attacks.

RECOMMENDATIONS

India needs legal instruments to have more effective cooperation abroad in the fight against cybercrime, underpinned by AI. That includes treaties and agreements focused on responding to an AI-enabled attack against the systems or other cooperation agreements with foreign jurisdictions having matters of extradition and prosecution in focus.There ought to be a special regulatory body put in place that monitors, supervises, and enforces the ethical use of AI both within the private and public sectors particularly on the matters of cybersecurity threats presented by AI systems. Research activities should be carried out throughout countries to bring a unified law with respect to AI-related crimes which are in nearest danger to every country in the coming future.

- **Amendment of IT Act of 2000:** The IT, Act 2000 is being amended to address AI-related cybercrimes

in an effort to develop corporate responsibilities of companies having AI, ease international cooperation for concerted cross-border attacks, enhance reporting obligations, and imposition of stiffer penalties for non-compliance.

- **Model of Liability Attribution**: Thus, a liability attribution model must categorically attribute the liability towards AI-generated cybercrimes between AI developers, deploying organizations, and end users to guarantee accountability based on control and oversight over the activities of the system.
- **Cross-Border Legal Structure:** India has to come closer to other countries with treaties and agreements that will facilitate information sharing, joint investigations, and extradition for assaults involving AI worldwide to ensure various measures against AI-driven cybercrimes.
- **Mechanisms for Accountability and Transparency:** Strict transparency rules would mandate that every organization disclose the vulnerabilities and breaches of AI systems.

CONCLUSION

India needs to enact a specific, independent law that governs AI and its roles in ransomware attacks as well as phishing attacks. Such a sui generis law must specify the liabilities and guidelines for regulation and enforcement related to AI-driven crimes. Clarification and updating of the Information Technology Act 2000 to cover AI-enabled cybercrimes: It needs to think about both AI-based systems, which function autonomously, and cross-border jurisdictions in the event of liability arising from AI-related attacks. Cybersecurity tactics will also need to change with the advancement of AI, and AI-based defenses are increasingly assuming importance in counteracting such increasingly sophisticated threats. AI in opposition to AI Defenders will embrace AI-driven cyber security technologies as attackers use AI to conduct increasingly complex attacks. As a result, there will be an AI arms race in which adversaries and allies will continuously enhance their systems to outsmart one another. Liability attribution models should be invoked in determining responsibility for AI-enabled attacks: there might be a liability model that blames AI developers, users, or entities deploying AI for malicious purposes, depending on the circumstances.

REFERENCES

1. https://link.springer.com/chapter/10.1007/978-3-031-12419-8_1
2. https://pubs.aip.org/aip/acp/article-abstract/2519/1/030036/2828543
3. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003258100-3/phishing-evolves-analyzing-enduring-cybercrime-adam-kavon-ghazi-tehrani-henry-pontell
4. https://link.springer.com/article/10.1365/s43439-023-00094-x
5. https://ieeexplore.ieee.org/abstract/document/10467401/
6. https://www.researchgate.net/profile/Sonali-Yadav-6/publication/340999611_APPLICATION_OF_ARTIFICIAL_INTELLIGENCE_IN_FIGHTING_AGAINST_CYBER_CRIMES_A_REVIEW/links/5ea92ed945851592d6a860df/APPLICATION-OF-ARTIFICIAL-INTELLIGENCE-IN-FIGHTING-AGAINST-CYBER-CRIMES-A-REVIEW.pdf
7. https://ejournal.uinfasbengkulu.ac.id/index.php/mizani/article/view/3318
8. https://www.utica.edu/academic/institutes/cimip/Phishing_Evolves_Analyzing-the-Enduring-Cybercrime.pdf
9. https://www.csoonline.com/article/569617/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html

10. https://www.scielo.org.za/pdf/sajim/v23n1/01.pdf
11. https://www.europarl.europa.eu/topics/en/article/20221103STO48002/fighting-cybercrime-new-eu-cybersecurity-laws-explained
12. Koops, E. J., and T. Robinson. "Cybercrime law: A European perspective." *Digital evidence and computer crime*. Academic Press, 2011. 123-183.
13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323258
14. https://lutpub.lut.fi/handle/10024/164184
15. https://search.proquest.com/openview/f50c69507802aace197ec39a079b92b8/1?pq-origsite=gscholar&cbl=2035897
16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3709095