Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries

Agus Nugroho1 · An An Chandrawulan1

Accepted: 24 August 2022 / Published online: 11 September 2022
© The Author(s), under exclusive licence to Springer Nature Limited 2022

Abstract
The COVID-19 pandemic poses an unprecedented global challenge to the whole society. Previously, most of the physical activities were not conducted online and were not exposed to cybercrime. Thus, it necessitates paying attention to this emerging phenomenon and devising strategies for a safe online environment for all stakeholders. The current study presents a historical overview of cybercrime and the cybersecurity system and highlights cybercrimes’ legal importance globally and cybercrime regulations during the Covid-19 times, specifically in the Indonesian context. Using a normative juridical approach, this study collected secondary data from various books, journals, regulatory guidelines, institutional reports, research, and the Internet. Additionally, a systematic literature search methodology was used to collect relevant secondary data from the most popular database, i.e., Scopus. Results revealed that although many nations are actively working to control cybercrimes, the issue persists, and many new cyber threats, i.e., scams and phishing, emerged during the Covid-19 pandemic. In such situations, along with the existence of a promising cybersecurity system, cybercitizens should always consider hygienic cyber tips to avoid being victims of cyber coronavirus crimes. Finally, after presenting an overview of the current state of cybercrime legislation on COVID-19, key policy recommendations for developed and developing countries are given, along with future research directions.

Keywords Cybercrimes · Cyber coronavirus crime · Laws and regulations · Covid-19 · Indonesia

Agus Nugroho
nugroho.agus.sik@gmail.com
An An Chandrawulan
ananchandrawulan@yahoo.com

1 Faculty of Law, Padjadjaran University, Sumedang, Indonesia
Introduction

The spread of COVID-19 worldwide led to a significant secondary threat to a technology-driven society. Since the outbreak, there have been reports of scams impersonating public authorities like WHO (Georgiadou et al. 2021) and organizations like supermarkets and airlines (Lallie et al. 2020), targeting support platforms (Sutherland 2021), conducting Personal Protection Equipment (PPE) fraud (Europol 2020), and offering COVID-19 cures (Fontanilla 2020). Besides, compared to the work environment IT devices, the devices at home are found to be poorly configured, thus making them highly susceptible to cyber-attacks (Saragih and Siahaan 2016). The increase in the use of these IT devices through the Internet has led to increased cybercrimes (Aizenkot and Kashy-Rosenbaum 2019). The crimes carried out with IT devices’ help, i.e., a computer, are termed Cybercrimes (Georgiadou et al. 2021). Moreover, the availability of the Internet is a prerequisite for such crimes. In addition, modern computerized technology and different software technical skills make individuals commit cybercrime. Cybersecurity experts estimate that the number of cybercrimes and attacks may have nearly doubled due to the COVID-19 pandemic (Horgan et al. 2021). Regardless of the world’s current situation, cybercriminals have seized the opportunity to attack individuals and organizations to steal sensitive information through various techniques. Hackers take advantage of the current pandemic uncertain situation to disseminate more distracting messages than usual, with varying sophistication degrees (Tan et al. 2020). Besides, cyber-attackers have targeted several critical infrastructures such as healthcare (Bernard et al. 2020).

In response to this, on April 8, 2020, the United Kingdom’s National Cyber Security Centre (NCSC), Cybersecurity and Infrastructure Security Agency (CISA), and the United States Department of Homeland Security (DHS) published a joint advisory about the activities of the Advanced Persistent Threat (APT) groups and cyber-criminals to exploit the current COVID-19 pandemic (Lallie et al. 2020). Moreover, cyber-criminals, malware, communication, and phishing platforms were discussed. However, there is a paucity of research regarding the broader assessment of the wide range of attacks related to the pandemic. Likewise, the literature lacks evidence regarding an overview of the amendments in international laws and security systems to prevent cybercrimes and safeguard the different sectors of society at the individual and organizational levels (Buil-Gil et al. 2020). This urgent situation needs attention to introduce new laws or amend existing cybercrime regulations to respond to the need of time. Thus, this research advanced by providing this synthesis in a time of crises situation to help further the lawmakers respond to the emerging scenario.

Furthermore, in a contextual scenario, despite several cybersecurity laws in Indonesia, numerous cybercrime cases have been witnessed during Covid-19 (Sari et al. 2021). The vulnerability of Indonesian public personal data was also exposed in 2020. In April 2020, cybersecurity became a trending issue owing to a breach suffered by an Indonesian Human Rights Activist on the activist’s chat messaging application. The breach led to the distribution of messages from his
account, provoking a public disorder. As a result, the police detained the activist under the allegation of spreading a “prohibited message.” After the activist’s detention, it took a few days to be released after providing sufficient evidence that his account was compromised and its control taken by an unknown party. In August 2020, the social media account of a scientist and two prominent institutions’ websites were hacked by cyber attackers. i.e., on Wednesday, August 19, 2020, the Twitter account of an epidemiologist at the University of Indonesia (UI) named Pandu Riono was allegedly hacked on. Pictures were posted by the “handle, @drpriono,” with the target of damaging the reputation of prof. Pandu. Later, law-making authorities could secure the account on Sunday, August 23, 2020, and the posts were deleted. Prior to this, the potential COVID-19 vaccine developed by Surabaya-based Airlangga University was slammed by Prof. Pandu, stating that still clinical trials are required to authenticate it. Moreover, the website of a critical research center, “the Center for Indonesia’s Strategic Development Initiatives (CISDI),” resulted in the loss of important documents from its website, “cisdi.org.” Besides, civil groups have condemned all cyberattacks and demanded law enforcement agencies to take corrective measures in this regard. After a series of incidents, there continued to be information breaches among the public (Hashimoto 2021). Cases were endured mostly by Indonesian marketplace platforms, exposing a significant amount of their consumers’ data, including names, email addresses, and other identifying information (Sulistyawati et al. 2021).

All such incidents drive the improvement of personal data protection, privacy, and the cybersecurity regulatory framework. In connection with that, The National Police Chief in Indonesia issued several Secret Telegrams regarding law enforcement efforts to prevent the spread of Covid-19. The Secret Telegram Number 1100 handles crimes related to situations and opinions in cyberspace (Sari et al. 2021). But still, it needs to be controlled at a larger scale with strict punishments. There are several studies related to cyber crimes and cybersecurity systems in Indonesia. However, there exists a gap regarding the comprehensive study during the COVID-19 pandemic discussing the international and national laws regarding cyber-crimes in the Indonesian context. In addition, there is an immense need to gather all regulatory information on cybercrimes in one synthesis so that regulatory amendments and best regulatory frameworks can be shared across the globe among lawmakers for better cybersecurity outcomes. Therefore, this research aims to make an advance by bridging this research gap to target the following objectives;

• To present a historical overview of cybercrime and cybersecurity systems.
• Cybercrimes during coronavirus and its legal importance.
• To present a cybercrime research overview 2019–2020 (Covid-19 time).
• To present an overview of the cybercrime regulations in Indonesia on COVID-19.
• To present an overview of the current state of international cybercrime legislation on COVID-19.
• To suggest recommendations for advanced and developing countries along with a conclusion and future directions.
Literature review

Historical overview of cyber crime and cyber security system

The term ‘hacking’ originated at the Massachusetts Institute of Technology (MIT); when to identify clever pranks and computer shortcuts, novel techniques were applied along with hacking by students of MIT (Baheti and Gill 2011). Besides, studies on computers and cybercrimes have been published since the late 1960s and 1970s. This period is recognized as the third industrial revolution due to “Internet Communication Technology (ICT)” development and growing globalization, and industrialization. Moreover, the research studies related to hacking, identification of viruses, identity thefts, spyware, malware, distributed denial-of-service attacks (DDoS), ransomware, scareware, cyberterrorism, etc., can be seen since that third industrial revolutionary era (Amir et al. 2018; Zolfi et al. 2019). Furthermore, more access to the Worldwide Web and user-friendly technology since the 1990s resulted in more cybercriminal activities (Zhang et al. 2012). Cybercrime cannot be conceptualized in a single definition, rather, it is best considered “a collection of acts of misconduct based on the material offense object and modus operandi that affect computer data or systems” (Sussman and Pollack 1995, p. 73). Moreover, “the term cybercrime constitutes illegal acts where a digital device or information system is either a tool or target or a combination of both” (Tan et al. 2020, p. 75).

Besides, according to the World Economic Forum, since 2010, the era of the fourth industrial revolution has begun (Schwab et al. 2016), which brought remarkable changes in the cyber world with heightened criminal activities. Simultaneously, Schwab (2017, p. 121) defines this era “as one characterized by developing new technologies that unite the biological, digital, and physical worlds, with implications across industries, economies, and disciplines.” During this period, the term cyber-crimes started to be used interchangeably with e-crime, computer crime, high-tech crimes, electronic crimes, information age crimes, digital crimes, cybernetic crimes, etc. Nowadays, the latest advancements in ICT and hacker subculture’s growth have categorized hackers into more subdivisions based on different motives, affiliations, and specializations (Aizenkot and Kashy-Rosenbaum 2019).

As for the cybersecurity laws and regulations, the first country to introduce the last related to cybersecurity was Sweden, with the law called the “Swedish Data Act of 1973”, specifying data protection against all illegal uses exceeds to that data (Yazdanfar 2013). The United States of America followed Sweden in creating security bills concerning cybercrimes with the “Federal Computer Systems Protection Act of 1977”. This bill was considered a role model for the criminal legislation of the coming times (Roddy 1979). Afterward, different nations introduced different laws at the national–international level to curb the activities of cyber-criminals. These include the United Kingdom’s National Cyber Security Centre (NCSC), the United Nations Office on drugs and crimes, the Cybersecurity and Infrastructure Security Agency (CISA), the United States Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST), etc. (Kagita et al. 2020).
Cyber crime and its legal importance Covid-19 time

Cyber coronavirus crime refers to “an unlawful act or default, which involves the use of or relating to computers, computer networks, or virtual reality, especially the Internet where coronavirus or COVID-19-themed emails, websites, links, social media, and short message service (SMS) are used to lure cybercitizens or persons to defraud or attempt to defraud them or cause damage, which is an offense against the public and renders the cybercriminal or person guilty of the act and liable to legal punishment” (Eboibi 2020, p. 17). This indicates the use of coronavirus at the lure to enhance criminal activities regarding information technology to harm others by either stealing the information of others or causing reputation or financial losses to others. In short, all those cyber activities, the outcomes of which are problematic for society and can be considered liable to punishment, come under the span of cyber coronavirus crimes (Khushnud and Qingjie 2020).

Moreover, due to the different governments’ strict lockdown orders to reduce the coronavirus spread, most people had to work from their homes rather than rotted visiting their offices (Mansoor 2021). Thus, most workers have to spend much time with their computers or laptops during working hours while sitting at their home, which makes the whole system vulnerable to the cyber-attacks because of the lack of safety and security measures available at home compared to the organizations (Abukari and Bankas 2020). Consequently, cybercriminals capitalize on the opportunity to attack the person working from home while committing cyber coronavirus crimes by stealing valuable information or causing financial losses to such employees and organizations (Tan et al. 2020). Moreover, the anxiety related to the situation and depression due to the prolonged condition of COVID-19 further provided an edge to the cybercriminals to attack emotionally weak persons and get the benefits of the pandemic (Olofinbiyi and Singh 2020). Besides, cybercriminals also targeted people searching for medical supplies online to keep them safe from the virus; instead of going out into the market this way, cybercriminals looted many people’s money by posting fake medicines accounts on social media. There are many examples where people ordered several medicines, sanitizers, and protective masks and paid the money, but none has been delivered (Sari et al. 2021).

Moreover, cyber attackers have also targeted law enforcement agencies and government institutions through calls, emails, and phishing scams (Lallie et al. 2020). For multiple requests for charity donations and health security investments, other purposes have been placed by asking for the account numbers and the people’s passwords (Bernard et al. 2020; Biswal and Pani 2021). Consequently, new domain names, malware, and phishing with the subject of COVID-19 have been introduced by cyber criminals to attack people for criminal activities. Moreover, falsified coronavirus news has been spread by using the government officials’ email addresses and official websites by hacking those sites to distract the people and create chaos in the country and for the payment from different parties (Bernard et al. 2020). While taking advantage of COVID-19 pandemic circumstances, cybercriminals also tried to introduce different medicines stating that they are the best cure for the coronavirus by misguiding the masses.
Thus, it is of utmost importance to revise the cybercrime laws and legislation worldwide to deal with such unlawful activities to protect the masses from being victims of such criminal activities and eradicate the cyber coronavirus crime. For this purpose, many law enforcement agencies are actively participating in lessening criminal attacks and devising laws to punish the culprits involved in cyber coronavirus crimes. However, the process of making such laws and policies needs to be accelerated along with strict punishment procedures so that hackers must not dare to play with the resources and emotions of the citizens.

**Cyber crime research overview 2020–2021**

The issue of cybercrime activities is of significant importance among researchers as well. This study listed some important research conducted during 2020–2021 regarding cybercrime based on a systematic review (Table 1).

**Cyber crime regulations in Indonesia: pre and post COVID-19 scenario**

The emergence of cybercrime has become a threat to the government’s stability because it is difficult to compensate for crime techniques done with computer technology, especially the Internet and intranet networks. Therefore, the government needs to pay attention to the security side in utilizing information technology (Aizenkot and Kashy-Rosenbaum 2019). Besides, overcoming the security disturbance requires law, as the law is a tool to organize society and meet concrete needs in society (Warasih 2005). Moreover, the law aims to realize interpersonal peace of life, including interpersonal order and personal interest (Purbacaraka and Soekanto 1978). Simultaneously, the security and legal certainty in utilizing information technology need to get attention, and the legal approach must be applied (Ranathunga et al. 2018). In connection to that, In Indonesia, the following laws are prevailing regarding cybersecurity systems:

- Act No. 8 the Year 1997 on Company Documents, in particular; Article 12, explains that company documents in the form of microfilms and other media (storage devices, information that is not paper and has a security level that can guarantee the authenticity of transferred or transformed documents) is recognized as valid evidence and imposes plenty against cyber-attacks.
- Act No. 36 the Year 1999 on Telecommunications, including:
  - Articles 22 and 50 provide a criminal penalty for the conduct of the crime manipulating access to telecommunication networks.
  - Article 38 and Origin 55 provide a criminal penalty for those who cause physical and electromagnetic interference with telecommunications operations.
  - Articles 40 and 56 provide criminal penalties for intercepting information through telecommunication networks.
| Sr. no. | Title                                                                 | Authors(s)/year                     | Journal                                             | Findings                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | “Some cybersecurity hygienic protocols for teleworkers in COVID-19 pandemic period and beyond” | Abukari and Bankas (2020)           | International Journal of Scientific & Engineering Research | To address the dangers of cybercrime during COVID-19, the current study offered some hygienic protocols along with revealing some defects that needed to be addressed while desktop sharing and using VPN to curb the activities of the cybercriminals |
| 2      | “Covid-19 and the digital revolution”                                | Hantrais et al. (2020)              | Contemporary Social Science                        | The pandemic sport for the change in data collection techniques has been discussed in this study, along with the dissemination of the official statistics to handle the issues related to the health treatments during the pandemic has been discussed in this study. Moreover, the authors discuss the importance of ethical context in artificial intelligence to remain productive and workable during the pandemic |
| 3      | “The Role and Place of Covid-19: An Opportunistic Avenue for Exponential World’s Upsurge in Cyber Crime.” | Olofinbiyi and Singh (2020)         | International Journal of Criminology and Sociology | An Emergency Management approach for protecting global citizens from cyber attackers has been discussed in this study since the pandemic outbreak, considering the criminal activities carried out during the pandemic |
| 4      | “Cybersecurity and Privacy Impact on Older Persons Amid COVID-19: A Socio-Legal Study in Malaysia” | Tan et al. (2020)                   | Asian Journal of Research in Education and Social Sciences | This study was conducted in an Australian context, where laws and effective agenda to control cybercriminal activities and the restructuring measures to remain competitive have been discussed |
| Sr. no. | Title                                                                 | Authors(s)/year      | Journal                                                                 | Findings                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------|----------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5      | Our digital footprint under Covid-19: should we fear the UK digital contact tracing app? | Guinchard (2020)     | International Review of Law, Computers & Technology                    | The contributors to government surveillance have been identified in this study, and the loopholes in data protection laws were discussed. The authors also suggested the enforcement of “the General Data Protection Regulation (GDPR)” in the private sector to disrupt the prevailing private sector surveillance in the UK context |
| 6      | “Cybercrime and shifts in opportunities during COVID-19: preliminary analysis in the UK.” | Buil-Gil et al. (2020) | European Societies                                                      | The authors pointed out the incremental cybercriminal activities worldwide during the COVID-19 pandemic. The authors also discussed that the reason behind this is the stringent lockdown policies. Moreover, the authors identified that the victims of cybercrimes during COVID-19 as mostly individuals rather than organizations overall |
| 7      | “Re-territorializing the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing.” | (Horgan et al. 2021) | Journal of Criminal Psychology                                           | The authors discussed the changes that the pandemic brought in terms of routine activities and ecological context that further provided room to the cybercriminals to come forward and attack vulnerable individuals and organizations, resulting in the tremendous increase in cybercriminal activities |
| Sr. no. | Title                                           | Authors(s)/year | Journal                     | Findings                                                                                                                                                                                                 |
|--------|-------------------------------------------------|-----------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8      | “Cyber-Security, Privacy, and The Covid-19 Attenuation?” | Samar (2021)    | Journal of Legislation      | In this article, the author depicted the importance of knowing the right to privacy by the common people and all legal entities. The authors also highlighted the importance of the legal protection acts against cyber criminals and their activities and the communication of the same to the people regarding their rights against the cyber attackers for the legal actions to be taken |


• Act No. 19 of 2002 regarding Copyright, especially;
  (a) Article 1 Paragraph 8 explains that a computer program is a set of instructions embodied in the form of language, scheme, code, or another form which, when combined with media that a computer can read, will be able to make the computer work to perform special functions or to achieve specific results, including preparation in designing these instructions.
  (b) Article 30 stipulates that the copyright period for a computer program is valid for 50 years,
• “Act No. 20 the Year 2001 Concerning Amendment to Act No. 31 the Year 1999 concerning Eradication Criminal Acts of Corruption” explains that evidence shall not only be obtained from the letters, statements of defendants, and the statements of witnesses, as provided for in the Criminal Procedure Code but includes other information that is said, sent, received or stored electronically (email), telegram, telex, fax, and from the document in any recording of data or information that can be issued with or without the aid of a means, whether contained on paper, any physical form other than paper, or electronically recorded, in the form of writing, sound, images, maps, designs of photographs, letters, signs, numbers, or perforations of meaning;
• Act No. 25 of the Year 2003 on Money Laundering, in particular.
  (a) Article 2 Paragraph 1 q explains the type of criminal fraud done through the Internet.
  (b) Article 38 letter b explains that the information uttered, transmitted, received, and stored electronically with optical instruments or similarly constitutes valid evidence.
• Act No 21 the Year 2007 on Trafficking in Persons in Part 29 provides evidence, information transmitted, spoken, received, stored electronically with optical devices or similarly, and recording data or information that may be viewed, read, be heard, and may be electronically recorded.
• Act No. 11, the Year 2008 on Information and Electronic Transactions, is expected to improve public services’ efficiency and effectiveness and open the widest opportunity to everyone optimally and responsibly. It is also expected to provide a sense of security, fairness, and legal justification for users and IT implementation. Positive law that can be used to handle cybercrime has been regulated in Act No. 11 the Year 2008, especially Article 27 to Article 52, is also regulated in other codes, namely: In the Criminal Code in particular Article 282 and Article 311 (dissemination of vulgar photos or film), Article 303 (on online gambling games), Article 331 (on defamation through the Internet), Article 335 (threats and extortion by email).

Along with the laws mentioned above, following ministerial regulations and guidelines are available in the Indonesian cybersecurity legal system.
• “Information Security Incident Response Team on Internet Infrastructure/Coordination Center (ID-SIRTII-CC) Ministry of Communications and Informatics.” To secure the telecommunication network, use the wild application of Internet protocols. This is based on “the Regulation of the Minister of Communication and Information Technology Number 16/PER/M.KOMINFO/10/2010”. Implementing the law enforcement process and the utilization of telecommunication networks to combat various possible threats and disturbances is the main objective of the ID-SIRTII-CC. It also aims to support coordination among the relevant parties abroad and at home to strategically detect, prevent, and mitigate the incidents.

• “Ministerial Regulation No. 82 of 2014; Ministerial Regulation No. 82 of 2014 of the Ministry of Defense” on cyber defense comprises the Cyber Defense guidelines, placed under the Indonesian National Armed Forces (TNI) authority.

• “Ministry of Communication and Information Technology Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (MCI 20/2016)”. These laws and regulations cover the general provisions on personal data processing requirements of electronic systems.

• State Cyber and Crypto Agency: It aims to Coordinate with “the Ministry for Political, Legal and Security Affairs, established by the Presidential Regulation N. 53 of 2017 (amended by Presidential Regulation N. 133 of 2017)”, took over the equipment, financing, archives and documents of “the State Encryption Agency’s,” “the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII),” and “the Information Security Directorate of the Ministry of Communications and Informatics” by taking the cybersecurity system implementation responsibility properly and efficiently. Moreover, it is mandated to manage national, regional, and international cooperation in cybersecurity affairs.

• “Government Regulation No. 71 of 2019 issued on Electronic System and Transaction Provision (GR 71/2019)” provides clearer obligations and rights to electronic system providers, including personal data processing.

• The Secret Telegram Number 1100 is regarding handling crimes related to situations and opinions in cyberspace while preventing the spread of Covid-19 issued by the National Police Chief.

As Indonesia’s positive criminal law is based on the provisions of the above-mentioned normative legislation, it is able to deal with the crime of misuse of information technology utilization (Sari et al. 2021). However, Ojiagu et al. (2020) argue that the Internet is only a method; the site can be seen as a house, and the data is the same as the property of a person; therefore, the law can be enforced to deal with the cybercrimes to protect the individuals as well as organizational privacy. Thus, there is a need to utilize all these laws and regulations to protect personal and organizational data and privacy and save citizens from becoming victims of fraudulent activities via electronic channels, especially during pandemic crises.
Research methodology

The research approach used is a normative juridical approach, with literature research examining the secondary data (Gaudêncio 2020). The current study used a descriptive-analytical method, which describes an ongoing condition or condition whose purpose is to provide data about the research object to explore and analyze the ideal constructs based on legislation (Mousavi et al. 2021). The data collection technique used by the authors in this research was the document study technique, which is a technique that studies various documents, especially legal documents related to Cybersecurity Law. This study uses secondary data from various books, journals, regulatory guidelines, institutional reports, research, and the Internet. Moreover, this research also used a systematic literature search methodology to collect relevant secondary data from the most popular database, i.e., Scopus. The keywords search was employed on the database using the most popular keywords such as “Pandemic 2019”, “COVID-19”, “Cybercrimes,” “Cyberattacks,” “Cybersecurity,” “Cybersecurity legislation,” “Cybersecurity laws,” “Cybersecurity regulations in Indonesia,” “Cybersecurity laws in Indonesia,” “Cybersecurity during Covid-19”. The timeline was selected from December 2019 to January 2021 to search cybercrimes, cyberattacks, and security system literature in the last 15 months. However, we acknowledge that some journals are excluded as a limitation of our methodical search using Scopus. The timeline search provided 37 articles broadly, which were further content analyzed by the study authors to select the eight most relevant studies to be included in this study, all of which were published in this 15-month (Feb-Sep, 2020) period of the COVID-19. Furthermore, the authors attempted to identify and address gaps in the literature and presented a consolidated review of the topic.

Results and discussion

Current international debate of cybercrime legislations during Covid-19 time

Cybercrime is a growing concern in countries worldwide. Around 154 countries (79%) have enacted cybercrime legislation; the pattern varies by region: Europe has the highest adoption rate (93%), and Asia and the Pacific have the lowest (55%) (Kinata 2016). During Covid-19, the evolving cybercrime landscape and resulting skills gaps are significant challenges for law enforcement agencies and prosecutors, especially cross-border enforcement. For many global policymakers, the pandemic’s transformative impact has reinforced the need to adopt new cybersecurity and privacy policies (Lu et al. 2021). These include efforts to promote data privacy and protection, raise baseline security standards of care, and implement cybersecurity certification regimes in 2021 and are;

- “National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity: The NIST, COVID-19 Cybersecurity Act, on August 11, 2020”. The provision of directions toas
higher educational institutions to mitigate the cybersecurity risks related to COVID-19 is among the NIST’s duties. Also, the recent cyberattacks on universities and colleges are being addressed by the officials directed in the bill.

- **The EU Commission** has launched a public consultation on a proposed revision of the NIS Directive entered into force in 2016. To clarify, cyber hygiene standards are among the public consultants’ main duties in the EU commission. They explain the expanded threat landscape arising from operational technology (OT) risks and cloud computing to harmonize security standards across the EU. Further, this harmonization can likely be achieved by implementing cybersecurity certification schemes via the UEU Cyber Security Act. Moreover, video cybersecurity authorities of the other member states like ANSSI in France and BSI in Germany are incorporating an important role in implementing these certifications in their respective countries working in line with the “European Commission and the European Agency for Network and Information Security (ENISA)” to drive towards greater convergence.

- **Brazil data security and Latin America regional influence** It has been more than 2 years since the “European General Data Protection Regulation (GDPR)” came into effect and changed the landscape of global data security. Nowadays, Brazil monitors this "data protection by default" approach of the GDPR with the “Lei Geral de Proteção de Dados Pessoais (LGPD),” dealing with a few major differences. The LGPD, effective in August 2020, applies to all Brazilian citizens’ data processors and organizations with a broader scope of application. Therefore, it is an efficient system to deal with criminals because it will be very difficult for them to understand the technicalities of this system and the plenty being imposed on cyber criminals. Moreover, being influential Across America, any security change in Brazil is expected to bring changes in the international security system.

- **Continued development of minimum data security standards** Regarding data security systems, various countries updated their regulations in 2020. These include Canada, Japan, India, Brazil, and New Zealand. All these countries follow the EU model of minimum cybersecurity system and, for non-compliance, impose substantial fines. This way of imposing cybersecurity systems with maximum part focusing on implementation is likely to reduce the intensity of cybercrimes in the near future (Devarapalli and Biswas 2021).

- **Focus on critical infrastructure and operational technology standards in APAC** Owing to most operational technology security policies across APAC, there arises a need to harmonize and implement the policies in the best possible way. There is a need for regional industrial groups to drive alignment with international consensus-driven standards to harmonize the whole process of the security system. For instance, “the ASEAN Ministerial Conference on Cybersecurity (AMCC)” agreed in 2018 to subscribe in principle to 11 non-binding voluntary norms by focusing on regional capability building and implementation of the same norms. Some of these norms include operational technology protection and critical infrastructure protection. In connection to that, in 2018, a master plan for OT standards was published by Singapore, which is now visible to grow across a PSC in the Year 2021 after the
increased OT threat landscape and development of the 5G technology all over the globe

- **Cybersecurity measures in Australia, India, and Japan** in 2020, Australia launched a consultation on a projected enhanced regulatory framework for functioning the national security system and infrastructure, which stems from the Australian Cyber Security Strategy 2020. Likewise, state leaders in India focus on the cybersecurity system to protect industries from cyberattacks. Thus, for India’s national cybersecurity strategy 2020, the cybersecurity systems enhancement and implementation. Moreover, Japan continues to implement provisions of “the Cyber-Physical Security Framework, released by the Ministry of Economy, Trade, and Industry (METI) in 2019” and focused on security for consumer and industrial IoT. As part of this implementation, METI released a draft IoT Security Safety Framework in 2020, focusing on security for the layer of mutual connections between physical devices and cyberspace.

- **Brexit and data security** The private privacy standards and enforcement of the security standards across the boundaries are the main aims of Brexit, which has been finalized with the UK and has been tested with new reviews and examination of data privacy enforcement and adherence to agreed-upon standards. While the UK has committed to implementing both the GDPR and the NIS Directive, data security remains a sensitive issue that the EU and UK governments will continue to review.

Moreover, business and security leaders can be prepared after understanding the policy landscape required to deal with cybercrimes and security issues. Nowadays, the universe is a global village; therefore, the policy strategies and laws in one region affect the policy strategies and laws in the other lead region along with the implementation of those laws (Chen et al. 2021). Moreover, data privacy and security are being scrutinized by most governments at a large level, which is likely to continue in the near future based on the situation in COVID-19. Hence, the government wants to be prepared for any uncertain situation in the future (Shinde and Kulkarni 2021). Therefore, the awareness of the above trends can further facilitate the leaders to stay connected with the government concerns that can further help them avoid unusual situations.

**Theoretical and practical implications**

**Recommendations for advanced and developing countries**

The current study review offers some valuable insights about cybercrimes and how these can be prevented. It also brings some recommendations for developing nations, including;

- Given the likely strain related to reactive and proactive law enforcement, it has been found that the prevailing system for investigating cybercrimes is not enough, which needs to be revised shortly to avoid any future consequences.
that arise during the pandemic, especially in the countries where resources are limited, and which are hit by the cyber criminals more intensely. This research attempts to generate awareness and significance of the topic at this crucial time of Covid-19.

- Governments need to communicate with the public regularly and should streamline the information provided to the public. As in times of uncertainty, citizens want immediate and accurate information about the prevailing circumstances. Whereas, in such situations, they believe immediately in what they can find due to their efforts, regardless of their authenticity. Also, in such circumstances, social media is considered the biggest source of information for the citizens of any country. Therefore, governments need to establish partnerships with social media players to reduce the cybercriminal activities spreading in the modern cyber world. Governments can also modify their outreach mechanisms to reduce the temptation to click on spurious links and email attachments. One option can be that they announce that all the sensitive information should not be revealed on the different platforms; the citizens should follow only one authentic platform to have authentic information regarding circumstances and important matters. Furthermore, that will be disseminated only from authorized government spokespersons, delivered at fixed times daily. This method might reduce some of the risks posed by phishing scams.

- The empowerment of vulnerable groups, especially children and seniors, is of utmost importance; therefore, public diplomacy and awareness should be given much weight to avoid vulnerable groups being the victims of cybercriminals. Accountable and transparent measures should be taken against those who are the reason for the misinformation or disinformation among the masses. On the other hand, source credibility should be given much importance. Sensitive information regarding cybersecurity threats must also be shared with the public by keeping the source of information secret because such kind of information helps those who are going to be the next victims of such attackers.

- Moreover, International examples of cyber-attacks and their cures can be discussed and shared with the citizens to benefit from other nations’ experiences because cyber crimes are boundaryless. The global cybercrime ecosystem is vast, but truly spectacular exploits are rare, and when they do occur, they grab the attention of other cyber criminals. This can generate a snowball effect within weeks or even days, as criminals rush to exploit a new vulnerability before cybersecurity experts can patch it.

- All measures used to counter cybercrime must continue to be proportionate, legal, accountable, and necessary. Many governments are using technology to assess, identify and trace potential COVID-19 patients. Now is the time to build cyber-confidence with the public and work together to counter the most pressing cybercrime threats and Covid-19 together.

- The introduction of the sensitization of cybersecurity programs in schools and workplaces can be an important step in protecting cyber citizens from attackers. As it has been found that the victim’s active participation is also an important part of a cybercriminal activity because it is the victim who allows the criminal to play with him/her. Therefore, cyber citizens will be better posi-
tioned to deal with such attackers once they are aware of the cyber scams and phishing emails. The World Economic Forum has estimated that the proportion of cyber-attacks that use social engineering like deception is as high as 98% (Shinde and Kulkarni 2021). Therefore, awareness among the masses needs to be created at the grassroots level to cross-check whether a message is genuine.

- Now is not the time to de-invest in specialist cybercrime law enforcement. To protect the Critical National Infrastructure, secure hospitals, empower industry, keep children safe online, and support economic recovery from COVID19, the building of the counter cyber-criminal capacity and capability is an important component. In this domain, most legislative activity can include measures like:

  i. government agencies must implement the necessary training and certain security policies to protect cyber citizens.
  ii. The government should also increase the penalties against those who commit computer crimes, e.g., ransomware.
  iii. within the insurance industry, the regulation of cybersecurity must be made mandatory to address the cybersecurity insurance issues
  iv. councils, commissions, or task forces can be created to spread awareness and advises on the cybersecurity issues
  v. supporting educational institutions and other institutions for conducting training and awareness programs regarding cybersecurity system

- At present, for the nations which do not have an overarching personal data protection law or where regulations on personal data protection are scattered within several sectoral laws and regulations, it is required by the governments and law enforcement agencies to present and pass an overarching personal data protection law to protect the masses from the intensity of cyber-attacks.

- The development dynamics of regulatory framework improvement cannot be separated from the role played by non-government entities. Therefore, civil society organizations (CSOs) need to advocate for the public’s interest by organizing a series of public awareness activities, conducting public surveys, facilitating dialogue with government and industry groups, and even filing lawsuits against the relevant courts. Self-regulatory industry groups also play a significant role in bridging the gap between industries’ best practices and regulations by creating industry codes of conduct and often meeting with regulators to expedite the war against cyberattacks. Thus, the involvement of multi-stakeholders in developing a regulatory framework on personal data protection, privacy, and cybersecurity is significant. However, it is indisputably important that every stakeholder educate the public on their rights to ensure any law can be implemented properly in practice. The right to privacy itself is not commonly known by the public in Indonesia.

- Thus, an inclusive and assertive legal approach is recommended for the legal system to amend and introduce laws related to cybercrimes and cybersecurity worldwide.
Strengths of the Study

This study is a unique attempt to summarise the contextual and international information related to cybercrime legislation during Covid-19. This study has summarised the 13 months of research on cybercrimes and Covid 19. This summary will help the field grow further, and future scholars may benefit from this research contribution. Moreover, this is a unique study that provides a historical overview of cybercrime and cybersecurity legislation from the beginning until 2021, advancing the existing literature on this topic. In addition, this study uniquely contributes to the body of knowledge by explaining the significance of cyber coronavirus crimes and generating awareness among lawmakers and government policymakers to grab their attention towards the emerging phenomenon as a societal issue. Besides, providing a detailed discussion about policies, regulations, laws, and legislations developed and implemented recently across the globe to respond to this emerging legal issue is another major advance of this research. It has provided a clear overview of all such measures together in one paper. Contextually, this research has made an advance by providing in-depth analysis and summarising the legal landscape of the Indonesian regulatory system regarding the Internet, ICT, cybercrimes, and cybersecurity. This synthesis will serve as a reference point for all future research attempts in this area. Hence contributing to the field growth for paving the way forward. Furthermore, this research has also provided legal and administrative recommendations for developing and developed countries to get key insights from these research findings. This is one of the major theoretical advances in the literature, which will open further avenues of debate in future research related to cybersecurity and cybercrimes.

Conclusion and future research directions

The outbreak of the COVID-19 pandemic has initiated several challenges among the nations worldwide regarding legislation and regulations; also, to curb the spread of the virus, most nations had to pose partial or full lockdowns all over the country. During such circumstances, where there was a kind of depression and anxiety among the people due to the vaccine’s unavailability and the continuous threat of COVID-19, the cybercriminals started to play their part while playing with the emotions and finances of the people. They started to place theme calls utilizing social media websites and SMS technology to spread fake news regarding the availability of the vaccine while attacking those who were more conscious about their health and hygiene, thus committing cyber coronavirus crimes. These cyber coronavirus crimes grew globally, and cyber citizens and the public have become exposed to higher risks. Consequently, there arises an immediate need for international device laws to curtail criminal activities and protect Internet users from cyber attackers; therefore, law enforcement agencies’ and prosecutors’ proactiveness is paramount. The collaboration of the law informs enforcement institutions and state agents inside and outside the state can be advantageous. Moreover, multiple measures can be taken for the proper investigation to identify and warn cybercriminals. For that, active campaigns must be launched against cybercrimes providing specific electronic information to
cyber citizens through various media to make them aware of cybercriminals’ intentions in acute circumstances.

Cybercitizens should always consider hygienic cyber tips to avoid being victims of cyber coronavirus crimes. In addition to being supported by the existing legal structure, the obstacles, i.e., electrical evidence factor, factor of the weakness of mastery information technology and its equipment for law enforcement, facilities, and infrastructure factor, the factor of difficultness is to present the victim, the factor of the weakness of public legal awareness must be overcome at the national and local level to ensure the enforcement of the laws to garb their benefits. Furthermore, future cybercrime research challenges lie in the changing landscapes of the Internet, virtual technologies, and law enforcement. Ordinary people are less aware of the modern forms of the crimes arising in today’s cyber world; therefore, they should be given proper training via different media channels to make them alert to the criminal activities of the cyber attackers (Arief et al. 2015), as the probability of becoming a victim can be reduced by spreading the information regarding new techniques of cybercrimes among cyber citizens.

Future research should also incorporate multimodal research techniques that apply quantitative, qualitative, and technological techniques to understand cybercrime better. International and interdisciplinary collaboration can also be facilitated to open new horizons and highlight cybercrime issues in the modern cyber world to protect the masses from the attackers’ criminal activities. In connection to that, academic institutions, corporate entities, private foundations, and government bodies should enhance the monetary funding available for young scholars to establish research projects that can spread enormous information regarding cyber criminal activities to the masses. Likewise, future researchers must not adopt the detective approach, but rather they should apply the preemptive approach to investigate, predict, and analyze the cause and consequences of cybercriminal activities using technical knowledge and transnational collaboration.

**Declarations**

**Conflict of interest** There is no conflict of interest among authors or with any third party regarding this manuscript.

**References**

Abukari, Arnold Mashud, and EdemKwedzo Bankas. 2020. Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *International Journal of Scientific & Engineering Research* 11 (4): 1401–1407.

Aizenkot, Dana, and Gabriela Kashy-Rosenbaum. 2019. Cyberbullying victimization in WhatsApp classmate groups among Israeli elementary, middle, and high school students. *Journal of Interpersonal Violence* 0886260519842860.

Amir, Eli, Shai Levi, and Tsafir Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies* 23 (3): 1177–1206.

Arief, Budi, MohdAzeem Bin. Adzmi, and Thomas Gross. 2015. Understanding cybercrime from its stakeholders’ perspectives: Part I–attackers. *IEEE Security & Privacy* 13 (1): 71–76.
Baheti, Radhakisan, and Helen Gill. 2011. Cyber-physical systems. *The Impact of Control Technology* 12 (1): 161–166.

Bernard, Rose, Gemma Bowsher, and Richard Sullivan. 2020. Cyber security and the unexplored threat to global health: A call for global norms. *Global Security: Health, Science and Policy* 5 (1): 134–141.

Biswal, Chandra Sekhar, and Subhendu Kumar Pani. 2021. Cyber-crimp prevention methodology. *Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications* 291–312.

Buil-Gil, David, Fernando Miró-Llinares, Asier Moneva, Steven Kemp, and Nacho Díaz-Castaño. 2020. Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies* 1–13.

Chen, Chao, Changjun Li, Genserik Reniers, and Fuqiang Yang. 2021. Safety and security of oil and gas pipeline transportation: A systematic analysis of research trends and future needs using WoS. *Journal of Cleaner Production* 279: 123583.

Devarapalli, Ravi Kishore, and Anupam Biswas. 2021. Rumor detection and tracing its source to prevent cyber-crimes on social media. *Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications* 1–30.

Eboibi, Felix E. 2020. Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures. *Commonwealth Law Bulletin* 1–30.

Europol. 2020. Pandemic profiteering: how criminals exploit the COVID-19 crisis.

Fontanilla, Marites V. 2020. Cybercrime pandemic. *Eubios Journal of Asian and International Bioethics* 30 (4): 161–165.

Gaudêncio, A.M.S. 2020. Rationality and/as reasonableness within formal-theoretical and practical-dialectical approaches to adjudication: Semiotic and normative perspectives. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique* 33 (4): 1033–1041.

Georgiadou, Anna, Spiros Mouzakitis, and Dimitris Askounis. 2021. Designing a cyber-security culture assessment survey targeting critical infrastructures during Covid-19 Crisis. *arXiv preprint arXiv: 2102.03000*.

Guinichard, Audrey. 2020. Our digital footprint under Covid-19: should we fear the UK digital contact tracing app? *International Review of Law, Computers & Technology* 1–14.

Hantrais, Linda, Paul Allin, Mihalis Kritikos, Melita Sogomonjan, Prathivadi B Anand, Sonia Livingstone, Mark Williams, and Martin Innes. 2020. Covid-19 and the digital revolution. *Contemporary Social Science* 1–15.

Hashimoto, Naofumi. 2021. Advocacy of cyber public health. *Global Health & Medicine* 2020.01105.

Horgan, Shane, Ben Collier, Richard Jones, and Lynsay Shepherd. 2021. Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology*.

Kagita, Mohan Krishna, Navod Thilakarathe, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, and Saurabh Singh. 2020. A review on cyber crimes on the internet of things. *arXiv preprint arXiv:2009.05708*.

Khushnud, Ziyodillioev, and Zhou Qingjie. 2020. Study on banks’ risk assessment of financing smallmedium enterprises’ project: The findings and experience from Uzbekistan banking sectors. *International Journal of Business and Administrative Studies* 6 (2): 86–96.

Kinata, Edric Julio. 2016. The effect of market volatility and firm size towards the difference of market reaction around stock-split announcement in Indonesia stock exchange. *Journal of Administrative and Business Studies* 2 (6): 304–313.

Lallie, Harjinder Singh, Lynsay A Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2020. Cyber security in the age of covid-19: A timeline and analysis of cyber-crimp and cyber-attacks during the pandemic. *arXiv preprint arXiv:2006.11929*.

Lu, Kaili, Harrison H. Yang, Yinghui Shi, and Xuan Wang. 2021. Examining the key influencing factors on college students’ higher-order thinking skills in the smart classroom environment. *International Journal of Educational Technology in Higher Education* 18 (1): 1–13.

Mansoor, Mahnaz. 2021. Citizens’ trust in government as a function of good governance and government agency’s provision of quality information on social media during COVID-19. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2021.101597.

Mousavi, S.A., G.H. Masoud and M. Raei. 2021. Analytical mechanisms in international documents and domestic laws and regulations. *Journal of Comparative Law* 8 (1): 253–282.
Ojiagu, Nkechi Cordelia, Hope Ngozi Nzewi, and Augustine Ebuka Arachie. 2020. Accountability and transparency in nation building: A covid-19 experience in sub-Saharan Africa. *International Journal of Public Policy and Administration Research* 7 (1): 23–33.

Olofinbiyi, Sogo Angel, and Shanta Balgobind Singh. 2020. The role and place of Covid-19: An opportunistic avenue for exponential world’s upsurge in cyber crime. *International Journal of Criminology and Sociology* 221–230.

Purbacaraka, Purnadi, and Soerjono Soekanto. 1978. *Renungan Tentang Filsafat Hukum*: Lembaga Penelitian Hukum, Fakultas Hukum Unsr.

Ranathunga, G.M., P.V.M. Karunaratne, and S.S.V. De Silva. 2018. Headress: Faith and practice in everyday life in Buddhism (The case of the temple of the tooth Buddhist religious activities and the cultural headdress of Sri Lanka). *Journal of Advanced Research in Social Sciences and Humanities* 3 (5): 172–178.

Roddy, John. 1979. The federal computer systems Protection Act. *Rutgers J. Computers Tech. & l.* 7: 343.

Samar, Vincent J. 2021. Cyber-security, privacy, and the Covid-19 attenuation? *Journal of Legislation* 47 (1): 1.

Saragih, YasmirahMandasari, and AndysahPuteraUtama. Siahaan. 2016. Cyber crime prevention strategy in Indonesia. *SSRG International Journal of Humanities and Social Science* 3 (6): 22–26.

Sari, Dewi Kartika, Jamilah Ahmad, Putri Hergiansari, Pratiwi Cristin Harun, and Nur Aji Wibowo. 2021. Quantitative study of the cyber-nationalism spreading on twitter with Hashtag Indonesia and Malaysia using Social Network Analysis.

Schwab, Klaus. 2017. *The fourth industrial revolution*. Currency.

Schwab, Stefan, Bernd Holzmüller, and Sören Hohmann. 2016. Automated verification of switched systems using hybrid identification. International Workshop on Design, Modeling, and Evaluation of Cyber Physical Systems.

Shinde, Nivedita, and Priti Kulkarni. 2021. Cyber incident response and planning: A flexible approach. *Computer Fraud & Security* 2021 (1): 14–19.

Sulistyawati, Sulistyawati, Rohkgmayanti Rohkmayanti, Budi Aji, SiwiPramatama Mars. Wijayanti, SitiKurniaWidi. Hastuti, Tri Wahyuni Suksesi, and Surahma Asti Mulasari. 2021. Knowledge, attitudes, practices and information needs during the COVID-19 pandemic in Indonesia. *Risk Management and Healthcare Policy* 14: 163.

Sussman, Vic, and Kenan Pollack. 1995. Gold rush in cyberspace. *US News and World Report* 13: 72–74.

Sutherland, Karen E. 2021. Managing reputation, ethics, risk, issues and crises. In *Strategic social media management*, 41–73. Springer.

Tan, SweeLeng, Rossanne Gale Vergara, Nasreen Khan, and Shereen Khan. 2020. Cybersecurity and privacy impact on older persons amid COVID-19: A socio-legal study in Malaysia. *Asian Journal of Research in Education and Social Sciences* 2 (2): 72–76.

Warasih, Esmi. 2005. telaah Sosiologis, Pranata Hukum–Sebuah, PT Suryandaru Utama, 2005. Semarang.

Yazdanfar, Darush. 2013. Profitability determinants among micro firms: evidence from Swedish data. *International Journal of Managerial Finance*.

Zhang, Yanping, Yang Xiao, Kaveh Ghaboosi, Jingyuan Zhang, and Hongmei Deng. 2012. A survey of cyber crimes. *Security and Communication Networks* 5 (4): 422–437.

Zolfi, Hamid, Hamidreza Ghorbani, and M Hossein Ahmadzadegan. 2019. Investigation and classification of cyber-crimes through IDS and SVM algorithm. 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC).

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.