UNIVERSITY OF THE PHILIPPINES
CENTER FOR INTEGRATIVE AND DEVELOPMENT STUDIES

ISSN 2619-7278 (Print)
ISSN 2619-7286 (Online)

Policy Brief
2024-06

PROGRAM ON SOCIAL AND POLITICAL CHANGE

Rethinking the Cybercrime Prevention Act of 2012

Strengthening Philippine Sovereignty in the Digital Age

Maria Corazon C. Reyes[1]

The Cybercrime Prevention Act of 2012 is a crucial step towards addressing cyber threats, but it faces significant issues that limit its effectiveness. Broad and vague provisions, technical and resource limitations, jurisdictional challenges, privacy and surveillance concerns, underreporting, international legal complexities, lack of specialized units, and the evolving nature of cyber threats all undermine the current framework. The recent incidents of cyberattacks targeting national government websites and institutions underscore the necessity of a comprehensive review of existing provisions.

In what ways does the current legal framework fall short in regulating cyber risks? Modern technologies constantly shift the environment for these threats, such as information hacking, deep fakes, and artificial intelligence. How effective is the current framework against these complex dangers? What are the key challenges faced by law enforcement agencies? How do the vague provisions of the law lead to potential overreach and arbitrary enforcement?

This policy brief evaluates the current cybercrime law's effectiveness in combating new and complicated cyber threats. Specific reforms are proposed to maintain the legislation's relevance. This brief also traces the Act's development and critically assesses its provisions, goals, and definitions against these emerging crimes. As such, this paper additionally examines the increasing incidence of cybercrimes in the Philippines since the law's enactment.

The brief recommends potential amendments to the Act, including redefining cybercrime offenses, updating investigative powers, and enhancing educational outreach. Existing provisions must also be reassessed. This reexamination is essential in strengthening Philippine sovereignty in the digital age.

Inception of Cybercrime Legislation

The United Nations General Assembly Resolution 53/70 of 1998, also known as the "Developments in the field of information and telecommunications in the context

[1] Maria Corazon C. Reyes (pspc.cids@up.edu.ph) is the Senior Project Assistant of the Program on Social and Political Change (PSPC) of the University of the Philippines Center for Integrative and Development Studies (UP CIDS). The program aims to develop a better understanding of past, current, and future sociopolitical tensions that can arise from and impact modern Philippine society and polity.

of international security," is a significant precursor to laws against cybercrime in many countries. This resolution urged member states to collaboratively assess existing and potential risks on information security. It also acknowledged concerns on the global impact of technologies, specifically on their possible misuse and the threats they may pose to international defense.

In the Philippines, there is an existing law against crimes for telecommunications technology: the Anti-Wiretapping Act, or the Republic Act No. 4200 of 1965. The principal objective of the Act is to safeguard the confidentiality of communication and to prohibit the unauthorized interception of private conversations. However, it is unsuitable to the challenges posed by the Internet in the 1980s.

In 1998, Republic Act No. 8484, or the Access Devices Regulation Act, grappled with the issue of fraudulent activities involving access devices, such as credit cards and ATM cards. Although the Act offered protection against banking fraud, its limited scope did not cover the range of fraud that emerged with e-commerce in the 2000s.

Republic Act No. 8792, also known as the Electronic Commerce Act of 2000, established the legal framework for electronic transactions and records in commercial and non-commercial settings. The serious harm that the ILOVEYOU virus inflicted in 2000 validated the necessity of this legislation.[2] Although the Philippines implemented the E-Commerce Law in June 2000, it could not be applied retroactively to prosecute the virus' creator due to the timing of the law's enactment (Romero 2012). The first conviction under this law occurred in 2005 when JJ Maria Giner became the first Filipino to face legal consequences. Giner was found guilty of unauthorized intrusion into computer systems, compromising the security of government websites such as "gov.ph." The case was significant as it marked a milestone after Giner was prosecuted under section 33a of RA 8792 (Sosa 2009, 83). However, the law remained insufficient in prosecuting specific attacks like hacking.

Cybercrime legislation eventually developed to address Internet crimes in the 2000s. This development was partly driven by international pressure to align with global standards such as the Budapest Convention, or the Convention on Cybercrime.[3] The legislation was drafted in 2001. The Cybercrime Prevention Act was then submitted to the Senate on 3 May 2011. Senate Bill No. 2796 reflects a collaborative legislative process in which senators proposed the consolidation of multi-authored, cybercrime-related bills into one comprehensive law. Authors included Edgardo J. Angara, Juan Ponce Enrile, Antonio Trillanes, Jinggoy Ejercito-Estrada, Lito Lapid, Manny Villar, Ramon Revilla Jr., and Miriam Defensor-Santiago.

RA 10175 or the Cybercrime Prevention Act of 2012

The Act took nearly eleven years to develop (Romero 2012). This lengthy process was pushed by the rise of social media and by public calls for stronger cybercrime legislation in the Philippines.

Moreover, Filipinos were increasingly becoming victims of cybercrime through social media (Avendaño 2013). Although the bill was approved by the House of Representatives, it faced delays in the Senate because of the electoral season. The Act was eventually enacted in 2012 (Franco and Su Yin 2012).

Between 2012 and 2020, the country witnessed significant cybercrime prosecutions. The Rappler Cyber Libel Case (2017–2020) was among the most high-profile ones (Jennings 2020). This culminated in the conviction of Maria Ressa, CEO of Rappler, and former researcher-writer Reynaldo Santos Jr. Their prosecution was based on a news article that Rappler published in 2012, in which businessman Wilfredo Keng was implicated in illicit activities, such as links to drug trade and human trafficking. Keng was prompted to file a complaint when

[2] The ILOVEYOU virus is a computer worm that infected millions of Windows computers globally in 2000. The virus, which spread through email attachments disguised as a love letter, caused billions' worth of damages to businesses and institutions, including Ford, the Pentagon, and the British Parliament. It was coded by Onel de Guzman, a 23-year-old Filipino.

[3] The Convention on Cybercrime, also known as the Budapest Convention, is the first international treaty that offers a practical framework to address cybercrime. It sought to harmonize laws, improve investigative techniques, and foster international cooperation. Becoming a party member offers benefits, including a global network of contact points against cyber offenses.

the same article was updated in 2014. The case enacted the cyber libel provisions of RA 10175[4] (Buan 2018). In June 2020, the Manila Regional Trial Court (RTC) found Ressa and Santos guilty. Both were sentenced to a maximum of six years of imprisonment. They were also required to pay damages (P&L Law Firm 2020). As a result, RA 10175 became the primary legislation in addressing cyber libel cases. Critics have since argued that the law–is being abused to silence journalists and activists. While the Act aims to combat legitimate cybercrimes, its application has sparked debates about its impact on civil liberties, including freedom of the press. Indeed, safeguards are needed to prevent its misuse.

In 2016, the country witnessed a series of notable cyber incidents (Gonzales 2019):

- The Commission on Elections (COMELEC) website was defaced (Chi 2016);
- Stolen funds from the Bangladesh Bank heist were laundered through a Philippine bank and casinos (Venzon 2019); and
- A major data breach at the Land Transportation Office (LTO) exposed millions of personal records (Samaniego 2020).

Virtual attacks against critical government institutions also surged in 2023 (Ombay 2023):

- The Philippine Health Insurance Corporation (PhilHealth) suffered from a ransomware attack (National Privacy Commission 2023);
- The Philippine Statistics Authority's (PSA) data was breached (Mapa 2023); and
- The House of Representatives website was also compromised (Dela Cruz 2023).

Many of these attacks, which were reportedly traced to Chinese IP addresses, heightened concerns about foreign interference and the security of national digital assets.

A massive data breach compromised 817.54 gigabytes of sensitive information from various government agencies, including the Philippine National Police (PNP), the National Bureau of Investigation (NBI), and the Bureau of Internal Revenue (BIR) (Caliwan 2023). Such infiltration revealed the vulnerability of the state's cybersecurity infrastructure. It disrupted critical government services and also jeopardized the personal data of millions of Filipinos.

Currently, the Philippines faces a virtual landscape characterized by frequent and sophisticated attacks, often targeting government institutions. These incidents have exposed significant weaknesses in the nation's defenses and the present legislation.

Examining cybercrime terms and definitions in RA 10175

Since the enactment of RA 10175, the digital space has introduced complex threats that dispute the Act's definitions and provisions.

One of the law's primary limitations are its vague terms. While it addresses "illegal access," it does not explicitly mention "hacking," a term that has become synonymous with unauthorized entry into computer systems. Similarly, "data interference" covers viruses and data alteration, but it may not fully recognize the complexities of malware and ransomware attacks, which have become a prevalent form of cyber extortion.

There are also gaps in the Act's provisions on computer-related fraud. Although it covers scams and financial theft, it may not sufficiently resolve the increasingly personalized phishing attacks. The definition of "identity theft" may not encompass the theft of personal credentials, which is a common precursor to various cybercrimes. Most importantly, given the growing complexity of artificial intelligence in imitating real-life persons, the definition of "identity theft" might need to be reexamined.

The distribution of illegal content reveals another limitation. While the Act covers child sexual abuse

[4] On 19 January 2018, the National Bureau of Investigation (NBI) stated that Rappler could still face cybercrime charges, even if the law cannot be applied retroactively. NBI Cybercrime Division Chief Manuel Antonio Eduarte cited the "continuous publication" theory. This enabled Keng to file a complaint, since he possibly read the article after the cybercrime law was enacted ("NBI: Rappler Can Be Liable for Cyber Libel despite Non-Retroactive Law" 2018).

material and libel, deepfakes[5] and other forms of manipulated media present new challenges. Provisions may not include the potential harm caused by these technologies, which can be used to spread disinformation, manipulate public opinion, and perpetrate various forms of fraud. To illustrate these inadequacies, the following terms and descriptions are provided:

TABLE 1. RA 10175 TERMS AND ITS DEFINITIONS

OFFENSE/THREAT	IS IT COVERED BY RA 10175?	DESCRIPTION
Illegal Access	✓	Unauthorized entry into computer systems, networks, or devices.
Data Interference	✓	Introduction of viruses, malware, or unauthorized alteration/deletion of data.
Computer-Related Fraud	✓	Online scams, phishing, financial theft using computers as tools.
Identity Theft	✓	Stealing personal information (e.g., name, ID numbers, financial details) for fraudulent purposes.
Distribution of Illegal Content	✓	Primarily focused on child sexual abuse material and online libel.
Social Engineering	×	Psychological manipulation to trick individuals into revealing information or performing actions (e.g., spear phishing, smishing, pretexting).
Critical Infrastructure Attacks	×	Cyberattacks targeting essential services like power grids, water systems, transportation, etc. (zero-day exploits)
Cloud & Mobile Security Risks	×	Exploiting cloud services and mobile devices for data theft, surveillance, and/or unauthorized access.
Cryptocurrency[6] Crimes	×	Fraud, extortion, and money laundering schemes using cryptocurrencies.
AI-Powered Attacks	×	Use of artificial intelligence (e.g., deep fakes, automated hacking tools) to enhance cyberattacks.
Hybrid Attacks	×	Combining multiple cyber techniques (e.g., phishing with malware) for increased effectiveness.

■ Source: Author

[5] A portmanteau of deep learning and fake, "deep fakes" are a type of artificial intelligence that convincingly replicates the face, voice, and/or likeness of another person. These are often used for deceptive reasons, such as identity theft, extortion, and/or sexual misconduct.

[6] Cryptocurrency is a digital payment system in which advanced encryption enables unregulated virtual transactions anywhere in the globe. It does not require a central regulator such as banks and governments to send or receive payments.

Table 1 illustrates the specific terms within RA 10175 that disclose the law's deficiencies on cyber protection. These terms can be grouped into the following categories:

1. Technical Attacks

The Act struggles to encompass the complexities of modern threats, such as zero-day exploits[7] and Advanced Persistent Threats (APTs),[8] which can target critical infrastructure and sensitive data. Additionally, the widespread use of new technologies has expanded the attack surface, creating vulnerabilities that RA 10175 does not explicitly criminalize.

2. Social Engineering

The law overlooks human manipulation in the virtual space. This manipulation is often coupled with the technical vulnerabilities of the site or the user's device. The goal is to deceive individuals and gain unauthorized access into their virtual networks.

3. Emerging Technologies

Emerging technologies, such as deepfakes and AI-manipulated information, pose new complications. These technologies can be used for disinformation, harassment, and fraud.

4. Infrastructure and Systems

There are also amplified risks to critical infrastructure, like power grids, hospitals, and transportation systems, which are increasingly targeted by cybercriminals.

5. Financial Crimes

Another complication is the evolving nature of electronic threats, like ransomware and the use of blockchain (crypto, coins payment) systems, to facilitate illicit activities.

Moreover, there is a striking imbalance between punitive measures and preventive strategies. The law underscores punishment for cybercrime offenses but lacks proactive mechanisms for prevention, such as information dissemination and citizen education. While there are provisions for law enforcement and capacity-building for authorities, there are no guidelines that empower the public to protect themselves online. Currently, the educational component is delegated to the Department of Information and Communications Technology (DICT), through the National Cyber Security Plan 2023–2028. However, this is mostly targeted to professionals.

The Act's punitive characteristic is also a reactive approach. Penalties are necessary, but they do not resolve the root causes of cybercrime, such as the public's lack of awareness, inadequate security measures, and vulnerabilities in digital infrastructure. A proactive strategy may include the following: investing in cybersecurity, public education campaigns, and enhancing the ability of law enforcement to identify and stop cyber threats.

Furthermore, appointing the NBI and the PNP as the primary enforcers signals public alarm because of their punitive approach. Although the DICT already underscores educational initiatives to promote cybersecurity awareness, there is a need to re-evaluate the principal enforcers and their operations. The aim is to launch a proactive cybersecurity infrastructure and spur public consciousness.

---

[7] Zero-day exploits are cyberattacks that take advantage of software vulnerabilities before the creator/user becomes aware of such weaknesses.

[8] Advanced Persistent Threats (APTs) are protracted and highly specialized cyberattack campaigns on networks, typically those of businesses and government institutions, to steal sensitive data.

Recommendations

Evidently, the legal framework inadequately covers emerging cybercrimes. Data protection is now in place to mitigate risks to individuals, but it still falls short in addressing changing technology-enabled crimes. Thus, the 2012 Cybercrime Prevention Act must be broadened to include new threats from modern technologies, such as artificial intelligence, the Internet of Things (IoT), blockchain, etc. This may also require developing specific investigative techniques to combat these evolving threats.

Cybersecurity education is also crucial. The Act is originally founded on the principles of prevention. As such, the government must implement an exhaustive awareness program that is integrated into the basic education curriculum and disseminated through media.

Improving enforcement mechanisms is fundamental. Given the transnational nature of cybercrime, the law should strengthen collaborations with like-minded nations, like those between the DICT and Japan, and ASEAN nations. The DICT must participate in global cybercrime task forces and align its activities with global standards.

Lastly, it is equally imperative that any developments do not undermine civil liberties. Striking a balance between security and individual rights is essential for maintaining public trust and ensuring the law's effectiveness.

Acknowledgments

The author extends sincere gratitude to Dr. Rogelio Alicor L. Panao[9] for his invaluable feedback and insightful critique of this paper.

[9] Dr. Panao is the convenor of the Program on Social and Political Change (PSPC) of the University of the Philippines Center for Integrative and Development Studies (UP CIDS). He may be reached through pspc.cids@up.edu.ph.

BIBLIOGRAPHY

Avendaño, Christine. "87% of Filipino Internet users have been victims of cybercrimes–DOJ." *Inquirer Technology*. January 1, 2013. https://technology.inquirer.net/21557/87-of-filipino-internet-users-have-been-victims-of-cybercrimes-doj

Buan, Lian. "NBI: Rappler Can Be Liable for Cyber Libel despite Non-Retroactive Law." 2018. Rappler. January 19, 2018. https://www.rappler.com/philippines/194036-nbi-rappler-cyber-libel-retroactive.

Chi, Leisha. "Philippines elections hack 'leaks voter data.'" *BBC*. April 11 2016. https://www.bbc.com/news/technology-36013713

Council of Europe. "Convention on Cybercrime." European Treaty Series No. 185. November 23, 2001. Accessed April 13, 2024. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Caliwan, Christopher Lloyd. "PNP-ACG probes 'massive' data breach." *Philippine News Agency*. April 20, 2023. https://www.pna.gov.ph/articles/1199811

Dela Cruz, Raymond Carl. "DICT probes cyberattack of House of Representatives website." *Philippine News Agency*. October 16, 2023. https://www.pna.gov.ph/articles/1211881

"Decision in People vs. Reynaldo Santos, Jr., Maria Angelita Ressa and Rappler, re Online Libel (Full Text)." *P&L Law Firm*. June 15, 2020. https://pnl-law.com/blog/decision-in-people-vs-reynaldo-santos-jr-maria-angelita-ressa-and-rappler-re-online-libel-full-text/

Franco, Joseph and Su Yin, Yeap. "President Aquino and the 2012 Cybercrime Prevention Act." *East Asia Forum*. October 31, 2012. https://eastasiaforum.org/2012/10/31/president-aquino-and-the-2012-cybercrime-prevention-act/

Gonzales, Cathrine. "Cybercrime on the rise over the last 6 years." *Inquirer.net*. October 15, 2019. https://newsinfo.inquirer.net/1177832/cybercrime-on-the-rise-over-the-last-6-years

Jennings, Ralph. "Rare Cyber Libel Case Tests Fragile Media Freedoms in Philippines." *VOA News*. April 24, 2020. https://www.voanews.com/a/press-freedom_rare-cyber-libel-case-tests-fragile-media-freedoms-philippines/6188156.html

Mapa, Claire Dennis. "On the CBMS Data Breach." *Philippine Statistics Authority*. October 13, 2023. https://psa.gov.ph/content/cbms-data-breach

"News Releases - Executive Order No. 58: Adopting the National Cybersecurity Plan 2023–2028 and Directing the Implementation Thereof." *Presidential Communications Office*. April 6, 2024. https://pco.gov.ph/news_releases/executive-order-no-58-adopting-the-national-cybersecurity-plan-2023-2028-and-directing-the-implementation-thereof/.

Ombay, Giselle. "Cybercrime incidents in NCR up by 152% in 2023 —PNP." *GMA News Online*. July 9, 2023. https://www.gmanetwork.com/news/topstories/metro/875252/cybercrime-incidents-in-ncr-up-by-152-in-2023-pnp/story/

"Press Statement on Alleged PhilHealth Data Breach." *National Privacy Commission*. September 25, 2023. https://privacy.gov.ph/press-statement-on-alleged-philhealth-data-breach/

Republic Act No. 4200. "An Act to Prohibit and Penalize Wiretapping and Other Related Violations of the Privacy of Communication, and for Other Purposes." June 19, 1965. https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/2/4442.

Republic Act No. 8484. "An Act regulating the issuance and use of access devices, prohibiting fraudulent acts committed relative thereto, providing penalties and for other purposes." February 11, 1998. https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/2/4601

Republic Act No. 8792. "Electronic Commerce Act of 2000." *Official Gazette of the Republic of the Philippines*. June 14, 2000. [UC1] https://www.officialgazette.gov.ph/2000/06/14/republic-act-no-8792/.

Romero, Purple. "The road to the Cybercrime Prevention Act of 2012." *Rappler*. October 10, 2012. https://www.rappler.com/philippines/special-coverage/13901-the-road-to-the-cybercrime-prevention-act-of-2012/.

Samaniego, Art. "How hackers collected sensitive data from the Land Transportation Office." *Manila Bulletin*. November 14, 2020. https://mb.com.ph/2020/11/14/how-hackers-collected-sensitive-data-from-the-land-transportation-office/.

Senate of the Philippines. "Committee Report No. 30- Senate Bill No. 2796." Fifteenth Congress of the Republic of the Philippines, First Regular Session. May 3, 2011. https://dict.gov.ph/wp-content/uploads/2014/07/senate-bill-no-2796_cybercrime-prevention-act-of-2011.pdf

Sosa, Gilbert C. "Country Report on Cybercrime: The Philippines." *UNAFEI Work Product of the 140th International Training Course*, no. 79 (2009): 79–86. April 6, 2024. https://www.unafei.or.jp/publications/pdf/RS_No79/No79_12PA_Sosa.pdf

United Nations Digital Library. "Developments in the Field of Information and Telecommunications in the Context of International Security:: Resolution: 53/70 Adopted by the General Assembly," December 11, 2018. https://digitallibrary.un.org/record/1655670.

Venzon, Cliff. "Philippine court finds banker guilty over Bangladesh Bank heist." *Nikkei Asia*. January 10, 2019. https://asia.nikkei.com/Spotlight/Most-read-in-2019/Philippine-court-finds-banker-guilty-over-Bangladesh-Bank-heist

The UP CIDS Policy Brief Series

The UP CIDS Policy Brief Series features short reports, analyses, and commentaries on issues of national significance and aims to provide research-based inputs for public policy.

Policy briefs contain findings on issues that are aligned with the core agenda of the research programs under the University of the Philippines Center for Integrative and Development Studies (UP CIDS).

CENTER FOR INTEGRATIVE AND DEVELOPMENT STUDIES

Established in 1985 by University of the Philippines (UP) President Edgardo J. Angara, the UP Center for Integrative and Development Studies (UP CIDS) is the policy research unit of the University that connects disciplines and scholars across the several units of the UP System. It is mandated to encourage collaborative and rigorous research addressing issues of national significance by supporting scholars and securing funding, enabling them to produce outputs and recommendations for public policy.

The UP CIDS currently has sixteen research programs that are clustered under the areas of education and capacity building, development, and social, political, and cultural studies. It publishes policy briefs, monographs, webinar/conference/forum proceedings, and the Philippine Journal for Public Policy, all of which can be downloaded free from the UP CIDS website.

THE PROGRAM

The **Program on Social and Political Change (PSPC)** provides a platform for understanding the varied social and political challenges facing modern Philippine society and polity from a multidisciplinary perspective. In relation to this, the Program also designs empirical studies using a variety of methods and approaches which form the basis for policy inputs and discussions at the local, national, and international levels.

Editorial Board

Program Editors

Editorial Staff

Get your policy papers published. Download open-access articles.

The *Philippine Journal of Public Policy: Interdisciplinary Development Perspectives* (PJPP), the annual peer-reviewed journal of the UP Center for Integrative and Development Studies (UP CIDS), welcomes submissions in the form of full-length policy-oriented manuscripts, book reviews, essays, and commentaries. The PJPP provides a multidisciplinary forum for examining contemporary social, cultural, economic, and political issues in the Philippines and elsewhere. Submissions are welcome year-around.

For more information, visit cids.up.edu.ph. All issues/articles of the PJPP can be downloaded for free.

Get news and the latest publications.

Join our mailing list: bit.ly/signup_cids to get our publications delivered straight to your inbox! Also, you'll receive news of upcoming webinars and other updates.

We need your feedback.

Have our publications been useful? Tell us what you think: bit.ly/dearcids.

UNIVERSITY OF THE PHILIPPINES
CENTER FOR INTEGRATIVE AND DEVELOPMENT STUDIES
Lower Ground Floor, Ang Bahay ng Alumni, Magsaysay Avenue
University of the Philippines Diliman, Quezon City 1101

Telephone (02) 8981-8500 loc. 4266 to 4268
(02) 8426-0955

Email cids@up.edu.ph
cidspublications@up.edu.ph

Website cids.up.edu.ph