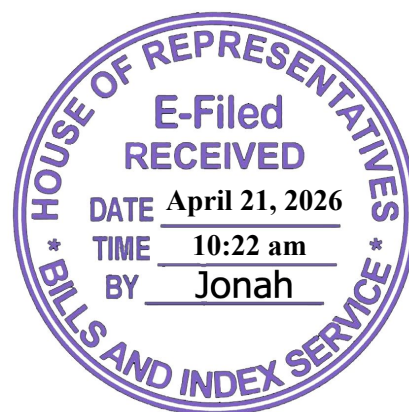




Republic of the Philippines
House of Representatives
Quezon City, Metro Manila

Twentieth Congress
First Regular Session

HOUSE BILL NO. **8910**



Introduced by Representatives Ferdinand Martin G. Romualdez, Yedda Marie K. Romualdez, Andrew Julian K. Romualdez, and Jude A. Acidre

AN ACT
STRENGTHENING THE CYBERCRIME PREVENTION MEASURES,
AMENDING FOR THE PURPOSE REPUBLIC ACT NO. 10175,
OTHERWISE KNOWN AS THE “CYBERCRIME PREVENTION ACT
OF 2012”

EXPLANATORY NOTE

Section 9, Article XIV of the 1987 Constitution mandates that the State shall promote the growth and generalized spread of technology and ensure that the benefits of science and technology are used to improve the productivity of the country. This constitutional directive necessitates a legal environment that is not only protective of digital infrastructure but also dynamic enough to respond to the rapid evolution of information and communications technology. Complementary thereto, Section 24, Article II recognizes the vital role of communication and information in nation-building, while Section 11, Article II mandates that the State value the dignity of every human person and guarantee full respect for human rights, which, in the digital age, includes the right to be secure in one’s electronic data and financial standing.

The Philippine agricultural and financial sectors remain the dual backbones of the national economy, yet they are increasingly vulnerable to a fragmented and evolving digital threat landscape. As of 2025, the Philippines has cemented its status as a global hotspot for cyber-attacks, ranking as the 3rd most targeted country for web threats globally. While the Information Technology and Business Process Management (IT-BPM) industry achieved historic success in 2025,

generating \$40.2 billion in export revenues and employing 1.9 million digital workers, this sector faces persistent and widespread computer-related fraud. These criminal activities resulted in estimated gross cyber losses of ₱5.82 billion in 2024 alone, threatening to erode investor confidence and hinder the industry's trajectory toward a projected \$42 billion in revenue by 2026.

Republic Act No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012," was enacted to safeguard the integrity of computer systems. However, as detected cyber threats have surged—with a staggering 71.9% increase in complaints recorded in early 2025—the limitations of the fourteen-year-old law have become apparent. Modern threats such as Advanced Persistent Threats (APTs), AI-driven phishing, and sophisticated social engineering schemes (which accounted for 76% of total fraud losses in 2025) now bypass the narrow definitions currently found in Sections 4(a)(3) and 4(b) of RA 10175.

This bill proposes to modernize our penal framework by widening the scope of computer-data-related offenses and allowing for the prosecution of key players, specifically targeting principals by inducement (the masterminds). By empowering parties who suffer direct or indirect damages to initiate prosecution, this measure ensures that technical loopholes do not become shields for criminals. These amendments are essential to ensuring the Philippines remains a competitive and secure hub for global business and a safer digital space for all Filipinos.

Similar bills were also filed during the 19th Congress.

In view of the foregoing, the passage of this bill is earnestly sought.



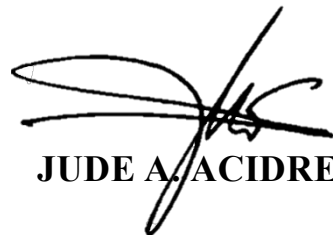
FERDINAND MARTIN G. ROMUALDEZ



YEDDA MARIE K. ROMUALDEZ



ANDREW JULIAN K. ROMUALDEZ



JUDE A. ACIDRE



Republic of the Philippines
House of Representatives
Quezon City, Metro Manila

Twentieth Congress
First Regular Session

HOUSE BILL NO. 8910

Introduced by Representatives Ferdinand Martin G. Romualdez, Yedda Marie K. Romualdez, Andrew Julian K. Romualdez, and Jude A. Acidre

AN ACT
STRENGTHENING THE CYBERCRIME PREVENTION MEASURES,
AMENDING FOR THE PURPOSE REPUBLIC ACT NO. 10175,
OTHERWISE KNOWN AS THE “CYBERCRIME PREVENTION ACT
OF 2012”

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

Section 1. – Section 3 of Republic Act No. 10175 is amended to read as follows:

“SEC. 3. *Definition of Terms.* – For purposes of this Act, the following terms are hereby defined as follows:

“(a) x x x;

x x x;

“(n) *Service provider* refers to:

“(1) x x x;[and]

“(2) x x x[-]; AND,

“(3) **ANY ENTITY CONTRACTED BY ANOTHER ENTITY, WHETHER DOMESTIC OR FOREIGN, TO**

PROCESS ANY DATA OR INFORMATION OF ANY PERSON WHEREVER LOCATED, INCLUDING ENTITY PROVIDING BUSINESS PROCESS OUTSOURCING AND SIMILAR SERVICES.”

“x x x;

“(o) *Subscriber’s information* refers to any information contained in the form of computer data or any other form that is held **OR ACCESSED** by a service provider, relating to subscribers, **WHETHER LOCATED IN THE PHILIPPINES OR NOT**, of its services other than traffic or content data and by which identity can be established:

“(1) x x x;

“(2) x x x;

“(3) x x x.”

“(p) x x x.

“(Q) *IDENTIFYING INFORMATION* REFERS TO ANY NAME OR NUMBER THAT MAY BE USED ALONE OR IN CONJUNCTION WITH ANY OTHER INFORMATION TO IDENTIFY ANY SPECIFIC INDIVIDUAL, INCLUDING ANY OF THE FOLLOWING:

“(1) NAME, DATE OF BIRTH, DRIVER’S LICENSE NUMBER, PASSPORT NUMBER, TAX IDENTIFICATION NUMBER, OR OTHER GOVERNMENT-ISSUED IDENTIFICATION NUMBER;

“(2) UNIQUE BIOMETRIC DATA, SUCH AS FINGERPRINT OR OTHER UNIQUE PHYSICAL REPRESENTATION;

**“(3) UNIQUE ELECTRONIC IDENTIFICATION
NUMBER, ADDRESS, OR ROUTING CODE; AND,**

**“(4) TELECOMMUNICATION IDENTIFYING
INFORMATION OR ACCESS DEVICE.”**

Section 2. – Section 4 of the same Act is amended to read as follows:

“SEC. 4. *Cybercrime Offenses.* – The following acts constitute the offense of cybercrime punishable under this Act:

“(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

“x x x

“(3) Data Interference. – The intentional or reckless alteration, **INPUTTING**, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses, **REGARDLESS OF WHO CONTROLS OR OWNS THE COMPUTER DATA.**

“x x x;

“(b) Computer-related Fraud. – The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing **ANY FORM OF damage, WHETHER DIRECT, INDIRECT, LEGAL, OR CONTRACTUAL**, thereby with fraudulent intent: *Provided*, That if no damage has been caused, the penalty imposable shall be one (1) degree lower.”

Section 3. – Section 5 of the same Act is amended to read as follows:

“SEC. 5. *Other Offenses.* – The following acts shall also constitute

an offense:

“(a) Aiding or Abetting in the Commission of Cybercrime. – Any person who willfully abets or aids in the commission of, **OR INFLUENCES OR DEVICES ANOTHER TO COMMIT** any of the offenses enumerated in this Act shall be held liable.

“(b) x x x.

“(C) **FAILURE TO SURRENDER COMPUTER DATA OR COMPUTER SYSTEM. – ANY PERSON WHO KNOWINGLY AND UNLAWFULLY POSSESSES OR FAILS TO SURRENDER ANY COMPUTER SYSTEM THAT CONTAINS COMPUTER DATA THAT ARE CONSIDERED PERSONAL INFORMATION, SENSITIVE PERSONAL INFORMATION, OR PRIVILEGED INFORMATION UNDER REPUBLIC ACT NO. 10173, OTHERWISE KNOWN AS THE “DATA PRIVACY ACT OF 2012,” SHALL BE HELD LIABLE.**

“(D) **SOLICITATION TO COMMIT CYBERCRIME. – ANY PERSON WHO WILLFULLY PROPOSES, SOLICITS, OR INDUCES ANOTHER PERSON TO COMMIT ANY OF THE OFFENSES UNDER THIS ACT SHALL BE HELD LIABLE.”**

Section 4. – Section 6 of the same Act is amended to read as follows:

“SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

“THE PROSECUTION OF THE OFFENSES UNDER THIS ACT MAY BE INITIATED BY ANY OFFENDED PART OR ANY AFFECTED SERVICE PROVIDER.”

Section 5. *Repealing Clause.* – All laws, presidential decrees or issuances, executive orders, letters of instruction, administrative orders, rules, or regulations contrary to, or inconsistent with the provisions of this Act, are hereby repealed, modified, or amended accordingly.

Section 6. *Effectivity Clause.* – This Act shall take effect after fifteen (15) days following its complete publication in the *Official Gazette* or in a newspaper of general circulation.

Approved,