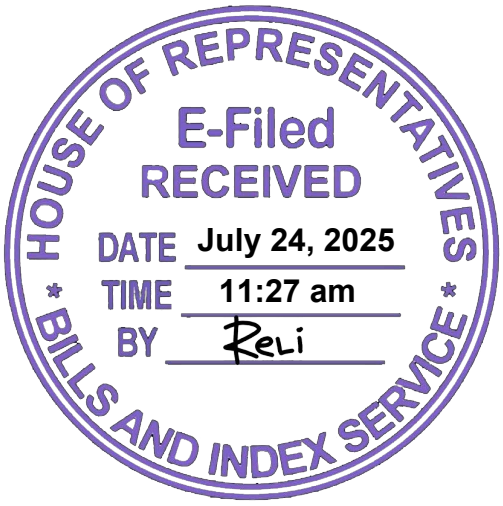
Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH (20th) CONGRESS
FIRST REGULAR SESSION

House Bill No. **2249**



Introduced by
Rep. ROBERT NAZAL

AN ACT
STRENGTHENING ACCOUNTABILITY FOR CYBERCRIMES PERPETRATED THROUGH THE USE OF DUMMY OR FICTITIOUS ONLINE ACCOUNTS, AMENDING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE "CYBERCRIME PREVENTION ACT OF 2012", AND ESTABLISHING COMPREHENSIVE MECHANISMS FOR CYBERCRIME PREVENTION, INVESTIGATION, PROSECUTION, AND VICTIM PROTECTION

EXPLANATORY NOTE

The rapid expansion of Philippine cyberspace has unleashed immense economic and civic potential. Yet, it has also opened the door to what the Philippine National Police Anti-Cybercrime Group (PNP-ACG) now identifies as the nation's "fastest-growing public-order threat." In 2024 alone, the PNP-ACG recorded 1,458 complaints of online libel, an average of nearly four per day and a 3.9 percent increase from the previous year, highlighting how reputational attacks flourish behind fictitious profiles. Identity theft follows a similar trajectory: 2,999 cases were reported in 2023, up 12.2 percent from 2022, with many traced to newly created sock-puppet accounts that vanish after illicit transactions.

Criminal anonymity exacts its highest toll on the vulnerable. An academic review of PNP records revealed a 30 percent increase in online human trafficking cases between 2019 and 2021, much of it tied to livestreamed cybersex operations orchestrated through burner social-media identities. Global data aligns, the 2022 Disrupting Harm report by ECPAT, INTERPOL, and UNICEF estimated that around two million Filipino children have already been exposed to online sexual abuse or exploitation, placing the Philippines at the epicenter of fake-account-driven predation.

While current laws penalize the consequences, libel, fraud, trafficking, and election violations, they fail to address the root tactic, which is the intentional use of dummy

accounts. The law does not currently recognize such use as a distinct crime or as an aggravating factor, nor does it require platforms to verify user identities or respond within defined timeframes when criminal content is reported. The SIM Registration Act of 2022 addressed mobile-related loopholes, but social media remains largely beyond its reach, leaving law enforcement to pursue digital phantoms across jurisdictions.

To preserve the promise of the digital age, we must close the anonymity gap without silencing legitimate dissent or whistleblowing. The proposed Cyber Crime Anti-Dummy Act of 2025 meets this need by legally defining “dummy accounts,” classifying their use as an aggravating circumstance, mandating 24- to 48-hour takedown and disclosure timelines for platforms, authorizing courts to issue Victim Protection Orders within 24 hours, and establishing a National Digital Forensics Task Force to enable swift, treaty-compliant evidence sharing. By aligning penalties with the scale of tech-enabled harm and enforcing greater platform accountability, this measure fulfills our dual constitutional duty: to uphold free expression and protect the public from abuse.

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

Rep. ROBERT NAZAL
Bagong Henerasyon Party-List

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH (20th) CONGRESS
FIRST REGULAR SESSION

House Bill No. **2249**

Introduced by
Rep. ROBERT NAZAL

AN ACT
STRENGTHENING ACCOUNTABILITY FOR CYBERCRIMES PERPETRATED THROUGH THE USE OF DUMMY OR FICTITIOUS ONLINE ACCOUNTS, AMENDING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE "CYBERCRIME PREVENTION ACT OF 2012", AND ESTABLISHING COMPREHENSIVE MECHANISMS FOR CYBERCRIME PREVENTION, INVESTIGATION, PROSECUTION, AND VICTIM PROTECTION

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

SECTION 1. SHORT TITLE.

This Act shall be known as the "Cyber Crime Anti-Dummy Act of 2025."

SECTION 2. DECLARATION OF POLICY.

It is hereby declared the policy of the State to foster an information and communications technology environment that promotes innovation and the free exchange of ideas while ensuring that such freedoms are not abused to the detriment of public order, economic security, individual rights, or the integrity of democratic institutions.

The State, therefore, commits itself to:

A. Deter, detect, and penalization of the creation and use of dummy, fictitious, or fraudulent online identities employed as instruments for the commission of crimes;

B. Impose corresponding obligations upon online service providers and internet intermediaries to prevent, mitigate, and remedy unlawful acts facilitated through their platforms;
C. Guarantee the prompt preservation of digital evidence and the expeditious disclosure of pertinent subscriber information when authorized by the court; and

D. Afford victims immediate and effective judicial relief without unduly restricting legitimate anonymity required for whistleblowing, journalistic investigation, or personal security.

SECTION 3. CONSTRUCTION AND INTERPRETATION.

The provisions of this Act shall be construed liberally in favor of protecting the public from cyber-enabled harm, which is consistent with the Bill of Rights and prevailing jurisprudence on freedom of expression, privacy, and due process.

SECTION 4. DEFINITION OF TERMS.

For the purpose of this Act:

A. Dummy Account - refers to any online persona, profile, or account, whether generated manually, algorithmically, or through artificial intelligence (AI), that includes the following:

    1. Created or operated using false, fictitious, or stolen personal information;
    2. Impersonates, mimics, or fabricates an identity with the intent to conceal the operator's true identity; or
    3. Employs automated bot networks, deep-fake technologies, or similar tools to mislead, defraud, threaten, harass, exploit, or otherwise facilitate the commission of an unlawful act.

B. Victim Protection Order (VPO) – refers to a summary and immediately executory order issued by a competent court directing the removal or disabling of specific online content, the preservation of electronic data, and the disclosure of subscriber or traffic data that are reasonably necessary to identify and locate the suspected offender

C. Platform Negligence – refers to the culpable failure of an online platform, service provider, or internet intermediary to act with reasonable dispatch, specifically, within forty-eight (48) hours upon valid notice of manifestly unlawful content or the confirmed existence of dummy accounts used in criminal activity

SECTION 5. CRIMINAL OFFENSES AND PENALTIES.

A. Any person who, through a dummy account, committed cyber libel as penalized under Section 4 (C, 4) of Republic Act No. 10175 shall suffer the penalty of imprisonment in its municipality's minimum period and shall pay a fine not exceeding One Million Pesos (PHP 1,000,000).

B. Any person who is found utilizing a dummy account, facilitates or commits any form of online sexual exploitation of children, as defined in Republic Act No. 11930 and other applicable statutes, shall suffer the penalty of reclusion temporal and shall pay a fine not less than Five Million Pesos (PHP 5,000,000).

C. Any person who is found utilizing a dummy account, organizes, recruits, transports, or benefits from human trafficking activities, in violation of Republic Act No. 9208 as amended by Republic Act No. 11862, shall be punished by reclusion perpetua and a fine of not less than Five Million Pesos (PHP 5,000,000).

D. Any person who is found utilizing a dummy account, disseminates false information, foreign-sourced propaganda, or coordinated inauthentic behavior to influence elections or sabotage the electoral process shall suffer the penalty of prision mayor in its maximum period to reclusion temporal, together with perpetual disqualification from public office, and the offense shall be non-bailable when funded, directly or indirectly, by any foreign principal.

E. Aggravating Circumstances. — The penalties prescribed in this section shall be increased by one-half (50%) when the following occurs:

    1. The victim is a minor;
    2. Deep-fake, synthetic media, or similar technologies are employed;
    3. The offense is carried out through a coordinated network comprising more than ten thousand (10,000) dummy accounts.

SECTION 6. CIVIL LIABILITY.

Independent of criminal liability, any person or entity found under this Act shall indemnify the aggrieved party for actual, moral, exemplary, and other damages under the Civil Code and applicable special laws.

SECTION 7. OBLIGATIONS OF ONLINE PLATFORMS AND INTERMEDIARIES.

A. Mandatory Identity Verification

    1. Basic Verification: All users seeking to open or maintain an account shall undergo at least a two-factor verification process, such as SMS or electronic

mail confirmation, pursuant to the National Privacy Commission Advisory on Identity Verification.

2. Enhanced Verification: Users who intend to purchase or place political advertising, render financial services, or distribute adult content shall, prior to activation of such functionality, submit a valid government-issued identification document or any equivalent credential recognized by law.

B. Notice-and-Action Regime: Upon receipt of a lawful order, takedown notice, or Victim Protection Order, a platform shall remove or disable access to the specified content, account, or data not later than twenty-four (24) hours from notice, extendible to forty-eight (48) hours upon a written showing of technical complexity.

C. Transparency and Accountability Reports: Every platform shall, within thirty (30) days after the close of each calendar quarter, submit to the National Privacy Commission a report indicating the following:

1. The aggregate number of dummy accounts detected and removed;

2. The number of takedown requests received, honored, or denied;

3. Other metrics to be prescribed by the Commission.

D. Administrative Sanctions: Any platform that willfully or negligently violates the obligations herein shall be penalized as follows:

1. First offense, a fine ranging from One Million Pesos (PHP 1,000,000) to Five Million Pesos (PHP 5,000,000) for each proven violation;

2. Subsequent offenses, a fine ranging from Five Million Pesos (PHP 5,000,000) to Twenty Million Pesos (PHP 20,000,000) and, upon recommendation of the National Privacy Commission and approval of the Department of Information and Communications Technology, temporary suspension or permanent blocking of its operations within the Philippines.

SECTION 8. INVESTIGATIVE POWERS AND EXPEDITED JUDICIAL PROCESSES.

A. Expedited Cyber Warrants

Judges designated to handle cybercrime cases according to Supreme Court Administrative Matters shall, upon receipt of a verified application demonstrating probable cause, resolve any petition for disclosure, search, seizure, or examination of computer data related to dummy accounts within seventy-two (72) hours.

B. National Digital Forensics Task Force

There is hereby created, under the administrative supervision of the Philippine National Police Anti-Cybercrime Group and in coordination with the National Bureau of Investigation, Department of Justice Office of Cybercrime, and Department of Information and Communications Technology, a National Digital Forensics Task Force that shall:

1. Maintain state-of-the-art forensic laboratories;

2. Coordinate with foreign law enforcement agencies under the Budapest Convention on Cybercrime and other mutual legal assistance treaties;

3. Train investigators, prosecutors, and judges in the handling of complex cyber-evidence.

SECTION 9. VICTIM PROTECTION ORDERS (VPO).

Any victim or duly authorized law-enforcement officer may file, ex parte or otherwise, a petition before the Regional Trial Court designated as a Cybercrime Court for the issuance of a VPO. Upon a finding of prima facie merit, the court shall issue the VPO within twenty-four (24) hours, which order shall be immediately enforceable.

SECTION 10. LEAD IMPLEMENTING AGENCY.

The Department of Information and Communications Technology shall be the primary implementing agency of this Act and shall, in coordination with the National Privacy Commission, the Department of Justice, the Department of the Interior and Local Government, and such other agencies as may be necessary, promulgate the requisite rules, regulations, and guidelines within thirty (30) days from the effectivity hereof.

SECTION 11. APPROPRIATIONS.

The amounts necessary for the initial implementation of this Act shall be charged against available appropriations of the concerned agencies. Thereafter, such sums as may be necessary for the continued implementation of this Act shall be included in the annual General Appropriations Act.

SECTION 12. IMPLEMENTING RULES AND REGULATIONS.

The Department of Information and Communications Technology, after public consultation and coordination with relevant stakeholders, shall promulgate the Implementing Rules and Regulations of this Act within thirty (30) days from its effectivity.

SECTION 13. REPEALING CLAUSE.

All laws, presidential decrees, executive orders, rules and regulations, or portions thereof that are inconsistent with any provision of this Act are hereby repealed, amended, or modified accordingly.

SECTION 14. SEPARABILITY CLAUSE.

If any section or provision of this Act is declared unconstitutional or invalid, the remainder thereof is not affected by such declaration and shall remain in full force and effect.

SECTION 15. EFFECTIVITY.

This Act shall take effect within fifteen (15) days after its complete publication in the Official Gazette or at least two (2) newspapers of general circulation.

Approved,