



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

Twentieth Congress
Second Regular Session



HOUSE BILL NO. 10309

Introduced by Representative Carlos A. Loria

EXPLANATORY NOTE

On June 22, 2026, two minor students perpetrated a shooting incident at San Jose National High School, Tacloban City. The Philippine National Police, Police Regional Office 5, has flagged this incident as part of a broader, highly localized digital-to-real-world security threat in which vulnerable Filipino youth are being radicalized online through Nihilistic Violent Extremism (NVE) — an ideology, spreading primarily through gaming platforms, online forums, and social media, premised on the belief that human life has no value.

Pursuant to the principle of *Parens Patriae* and the State's constitutional mandate to protect the physical, moral, spiritual, intellectual, and social well-being of the youth, government has both the authority and the duty to respond to this threat. That response, however, must be as carefully constructed as the threat is real. A regulatory scheme that criminalizes ordinary negligence, sweeps in legitimate expression, or authorizes platform blocking without judicial oversight risks being struck down — as the Supreme Court struck down a comparable blocking provision of the Cybercrime Prevention Act in *Disini v. Secretary of Justice* (G.R. No. 203335, February 18, 2014) — and risks doing little to actually protect at-risk youth in the meantime.

This bill accordingly reframes the original proposal along four lines. First, it confines criminal liability to persons who knowingly and intentionally propagate NVE, groom minors, or defy lawful orders, while routing negligent or merely non-compliant conduct through a proportionate administrative track. Second, it requires prior judicial authorization before any platform, domain, or IP address may be blocked, and builds in notice, an opportunity to cure, and a right to contest. Third, it pairs platform accountability with a genuine prevention architecture, digital literacy education, a 24/7 hotline, and referral of at-risk and radicalized minors to rehabilitative rather than punitive intervention, consistent with the Juvenile Justice and Welfare Act. Fourth, it protects the privacy of the very minors it aims to shield, by requiring that any age-verification scheme comply with the Data Privacy Act and collect no more data than necessary.

Hence, the passage of this bill is urgently sought to protect Filipino children from digital radicalization in a manner that is effective, proportionate, and constitutionally sound.


Carlos A. Loria



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

Twentieth Congress
Second Regular Session

HOUSE BILL NO. 10309

Introduced by Representative Carlos A. Loria

**AN ACT PROTECTING FILIPINO CHILDREN AND YOUTH FROM ONLINE
RADICALIZATION AND NIHILISTIC VIOLENT EXTREMISM, ESTABLISHING
A NATIONAL FRAMEWORK FOR PREVENTION, DUE-PROCESS-BASED
PLATFORM ACCOUNTABILITY, AND REHABILITATION, AND
APPROPRIATING FUNDS THEREFOR**

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 "Counter-Digital Radicalization of Youth Act."

SEC. 2. Declaration of Policy. — It is the policy of the State to protect and promote the physical, moral, spiritual, intellectual, and social well-being of children and youth, consistent with Article II, Section 13 and Article XV, Section 3 of the Constitution. Recognizing the principle of *Parens Patriae*, the State shall defend children from all forms of neglect, abuse, cruelty, exploitation, and other conditions prejudicial to their development, and shall aid parents in fulfilling this responsibility.

The State likewise recognizes that children and youth are rights-holders entitled to freedom of expression, access to information, and privacy in digital spaces, consistent with the Constitution, the United Nations Convention on the Rights of the Child, and Republic Act No. 7610. Towards this end, the State shall take proactive, evidence-based, and proportionate measures against online radicalization and Nihilistic Violent Extremism (NVE) that: (1) hold accountable those who deliberately exploit digital platforms to target, groom, or incite minors to violence; (2) require reasonable, privacy-respecting safeguards from service providers; (3) prioritize prevention, digital literacy, and rehabilitation over blanket prohibition; and (4) ensure

that any restriction on access to information or expression is narrowly drawn, subject to due process and judicial oversight, and no broader than necessary to address a demonstrable harm.

SEC. 3. Definitions. — As used in this Act:

- a) **Nihilistic Violent Extremism (NVE)** — refers to an ideology or belief system, propagated through digital means, premised on the notion that life has no inherent value or meaning, which actively encourages or incites an individual, particularly a minor, to commit acts of violence against themselves or others. It does not include the mere expression of nihilistic, existential, or fatalistic philosophical viewpoints absent a specific incitement or solicitation to violence.
- b) **Online Radicalization** — refers to the process by which an individual is gradually introduced to, and progressively adopts, extremist ideology, including NVE, through sustained exposure to online content, communications, or networks.
- c) **Age-Inappropriate Violent Content** — refers to digital games or interactive media that, based on generally accepted content-rating standards (such as the International Age Rating Coalition system or an equivalent classification recognized by the Movie and Television Review and Classification Board), are rated unsuitable for minors due to graphic, gratuitous, or realistic depictions of violence, and which are made accessible to minors without adequate Age Assurance.
- d) **Digital Grooming** — refers to the deliberate use of online platforms or communications to build a relationship of trust with a minor, or to manipulate, coerce, or psychologically condition a minor, for the purpose of inducing the minor to adopt violent extremist ideology or to commit an act of real-world violence.
- e) **Service Provider** — refers to any natural or juridical person, local or foreign, offering online gaming platforms, social media networks, hosting services, or other digital platforms accessible to users within the Philippines. For purposes of the graduated obligations under this Act, a service provider shall be classified as "large-scale" or "small and medium-scale" based on criteria — including average monthly active Filipino users and annual gross revenue derived from the Philippines — to be set by the Department of Information and Communications Technology (DICT) in the Implementing Rules and Regulations (IRR).
- f) **Age Assurance** — refers to a method or combination of methods used by a service provider to establish, with reasonable confidence, whether a user is a minor, using the least privacy-intrusive means reasonably available — such as age estimation, self-declaration paired with risk-based verification, or parental consent — and which shall

not require the collection or retention of government-issued identification except where no less intrusive method is reasonably available.

- g) **Minor** — refers to any person below eighteen (18) years of age, or one who, though over eighteen (18) years of age, is unable to fully take care of or protect himself/herself from abuse, neglect, cruelty, exploitation, or discrimination because of a physical, mental, intellectual, or sensory disability, condition, or impairment. For purposes of this Act, the term shall additionally include any individual, regardless of apparent or actual chronological age, who is presented, depicted, or portrayed as a minor within digital spaces or online platforms.
- h) **Trusted Flagger** — refers to an individual or organization accredited by the DICT, with demonstrated expertise in identifying NVE content or online radicalization, whose reports of prohibited content a service provider shall prioritize for review.
- i) **Competent Authority** — refers to the government agency or office vested with authority to implement a specific provision of this Act, as designated herein or in the IRR.

SEC. 4. Rule of Construction and Protected Content. — Nothing in this Act shall be construed to authorize the prohibition, censorship, or restriction of content on the basis of viewpoint alone, or to apply to bona fide news reporting, historical or documentary material, artistic, literary, or religious works, satire, or educational content, provided the same is not used as a means of Digital Grooming or deliberate incitement to violence as defined herein. Any restriction, takedown, or blocking order issued under this Act shall be narrowly tailored, shall employ the least restrictive means reasonably available, and shall be subject to the due-process safeguards under Section 8.

SEC. 5. Prohibited Acts. — The following acts, when committed knowingly and with intent, are hereby declared unlawful:

- a) **Deliberate Algorithmic Propagation of NVE** — Knowingly designing, configuring, or deploying an algorithm, forum, chatroom, or user-generated feature of a platform for the specific purpose of spreading, amplifying, or sustaining NVE content directed at minors;
- b) **Digital Grooming and Exploitation of Minors** — Using online platforms to target, manipulate, groom, or exploit a minor for the purpose of inducing the minor to adopt violent extremist ideology or to commit an act of real-world violence;
- c) **Commercial Distribution of Age-Inappropriate Violent Content to Minors** — The knowing and commercial hosting, offering, or distribution of Age-Inappropriate Violent Content directly to minors in the Philippines without implementing the Age

Assurance measures required under Section 6, after having received notice of non-compliance under Section 8 and failing to cure the violation within the period stated therein; and

- d) **Obstruction** — Knowingly obstructing, evading, or refusing to comply with a lawful summons, subpoena, or final order issued under this Act.

A merely negligent, inadvertent, or isolated failure to moderate content, absent the actual knowledge and intent required above, shall not give rise to criminal liability under this Section, but may constitute an administrative violation under Section 7.

SEC. 6. Mandatory Safeguards. — All service providers offering online gaming or social media platforms accessible in the Philippines shall:

- a) Implement reasonable, risk-based, and privacy-preserving Age Assurance measures proportionate to the risk of harm posed by the platform's content;
- b) Establish an accessible reporting mechanism through which users, parents, and Trusted Flaggers may flag suspected NVE content or signs of online radicalization, and review flagged reports within a reasonable period to be fixed in the IRR, which period shall be shorter for large-scale service providers;
- c) Provide parents and guardians with reasonably accessible parental control tools; and
- d) For large-scale service providers, publish an annual transparency report on content-moderation actions relevant to NVE and Age-Inappropriate Violent Content, consistent with Section 13.

A service provider that complies with this Section in good faith shall not, on that basis alone, expose itself or its officers to criminal liability.

SEC. 7. Administrative Violations and Enforcement. — Failure of a service provider to comply with Section 6, or to act on a valid notice issued under Section 8, shall constitute an administrative violation, without prejudice to any criminal liability that may separately arise under Section 5. The DICT, after notice and opportunity to be heard, may impose administrative fines of not less than One Hundred Thousand Pesos (PHP 100,000.00) nor more than Two Million Pesos (PHP 2,000,000.00) per violation, taking into account the gravity of the violation, the size and resources of the service provider, and whether the violation is a first or repeated offense. Administrative orders of the DICT may be appealed to the Court of Appeals without need of a supersedeas bond for a first-time violation.

SEC. 8. Notice, Takedown, and Blocking Procedure. —

- a) **Notice and Opportunity to Cure** — Before any content is ordered taken down or any platform, domain, or IP address is ordered blocked, the DICT or the Philippine National Police Anti-Cybercrime Group (PNP-ACG) shall issue written notice to the service provider identifying the specific content or violation and affording it a reasonable period, not exceeding seventy-two (72) hours, to take down the content or otherwise cure the violation, except as provided in subsection (c).
- b) **Judicial Authorization for Blocking** — Any order to block, restrict, or blackhole access to an entire platform, domain, or IP address shall require prior authorization from a designated Cybercrime Court, upon verified application showing probable cause that the platform is being used for a prohibited act under Section 5 and that blocking is necessary because less restrictive measures, including targeted content takedown, are inadequate. This safeguard reflects the constitutional guarantee of due process and the Supreme Court's ruling in *Disini v. Secretary of Justice* (G.R. No. 203335, February 18, 2014), which struck down a comparable blocking mechanism under Republic Act No. 10175 for lack of judicial oversight.
- c) **Emergency Takedown** — Where content poses an imminent risk to life, the Director of the PNP-ACG may issue an emergency takedown order effective for a period not exceeding forty-eight (48) hours, which must be confirmed by a Cybercrime Court within that period to remain in effect; otherwise, it shall automatically lift.
- d) **Right to Contest** — A service provider or content creator affected by an order under this Section may contest the same before the issuing authority or the Cybercrime Court, as applicable.

SEC. 9. Data Privacy and Protection of Minors' Information. —

Any Age Assurance mechanism or other data collection undertaken pursuant to this Act shall comply with Republic Act No. 10173 (Data Privacy Act of 2012). Service providers shall: (a) collect only the minimum personal data necessary; (b) not retain such data beyond the period necessary for the stated purpose; (c) not use data collected for Age Assurance for any other commercial purpose without separate, freely given consent; and (d) allow the National Privacy Commission to review compliance. The National Privacy Commission shall be consulted by the DICT in formulating the IRR governing Age Assurance.

SEC. 10. Prevention, Digital Literacy, and Education Program. — The Department of Education (DepEd), in coordination with the DICT and the Commission on Higher

Education (CHED), shall integrate age-appropriate digital literacy and online-radicalization awareness modules — including modules for parents and guardians — into the basic and tertiary education curricula within one (1) year from the effectivity of this Act.

SEC. 11. Referral, Diversion, and Rehabilitation Program. — Minors identified as being at risk of, or subject to, online radicalization shall be referred to the appropriate intervention and diversion programs of the Department of Social Welfare and Development (DSWD) and the mental-health services of the Department of Health (DOH), consistent with Republic Act No. 9344 (Juvenile Justice and Welfare Act of 2006), as amended. Nothing in this Act shall be construed to subject a minor who has been radicalized or exposed to NVE content to criminal liability under this Act on account of that exposure alone; intervention for such minors shall be rehabilitative, not punitive.

SEC. 12. National 24/7 Hotline. — The DICT, in coordination with the PNP and DSWD, shall establish and maintain a toll-free hotline and online reporting channel through which parents, guardians, educators, and minors may report suspected online radicalization or NVE-related content and obtain referral to appropriate support services.

SEC. 13. Inter-Agency Council Against Online Youth Radicalization. — There is hereby created an Inter-Agency Council Against Online Youth Radicalization (the "Council"), to be chaired by the DICT and co-chaired by the Department of Justice (DOJ), with the PNP, DepEd, DSWD, DOH, CHED, the National Privacy Commission, the National Youth Commission, and one (1) representative each from industry and civil society as members. The Council shall coordinate implementation of this Act, monitor emerging NVE trends, and submit an annual public report to Congress on its implementation, including the number and outcomes of takedown and blocking orders issued and their impact, if any, on lawful expression.

SEC. 14. Power to Issue Summons and Subpoenas. — To carry out investigations under this Act, the Director of the PNP-ACG, or a duly authorized representative, may issue administrative summons, subpoenas duces tecum, and subpoenas ad testificandum to compel the attendance of witnesses and the production of relevant server logs, operational data, and records from service providers, subject to the safeguards of Republic Act No. 10173. Non-compliance with a lawfully issued summons or subpoena shall constitute contempt and may ground the filing of appropriate obstruction charges before the proper court.

SEC. 15. Special Technical Powers of the DICT. — The DICT shall serve as the primary technical monitoring and regulatory authority under this Act and, subject to the procedure under Section 8, is hereby empowered to: (a) audit the systems of service providers

to verify compliance with Section 6; (b) issue takedown directives for specific NVE content or Age-Inappropriate Violent Content; and (c) petition the Cybercrime Court for an order blocking access to a platform, domain, or application operated by a non-compliant service provider.

SEC. 16. Special Legal and Prosecutorial Powers of the DOJ. —

The DOJ, through its Office of Cybercrime (OOC), shall serve as the central legal authority for enforcement and prosecution under this Act. The DOJ is hereby empowered to:

- a) **Prosecutorial Task Force** — Designate specialized cyber-prosecutors to lead the criminal prosecution of persons violating this Act;
- b) **Asset Forfeiture** — File civil and criminal forfeiture cases before the proper courts to freeze, seize, and confiscate digital assets, localized servers, domains, and financial proceeds derived from violations of Section 5; and
- c) **International Legal Cooperation** — Initiate international requests for Mutual Legal Assistance Treaties (MLAT), extradition, or cross-border data retention with foreign states to secure evidence, server data, and custody over foreign offenders.

SEC. 17. Penalties. —

- a) **Criminal Penalties** — Any person found guilty of committing an act prohibited under Section 5(a) or (b) shall suffer imprisonment of six (6) years and one (1) day to twelve (12) years, and a fine of not less than Five Hundred Thousand Pesos (PHP 500,000.00) nor more than Five Million Pesos (PHP 5,000,000.00), at the discretion of the court. Any person found guilty of committing an act prohibited under Section 5(c) or (d) shall suffer imprisonment of one (1) month and one (1) day to six (6) years, or a fine of not less than One Hundred Thousand Pesos (PHP 100,000.00) nor more than One Million Pesos (PHP 1,000,000.00), or both, at the discretion of the court.
- b) **Liability of Corporate Officers** — Where the offender is a juridical entity, criminal liability shall attach only to the officer or officers who had actual knowledge of, and directly participated in or consented to, the commission of the prohibited act. The mere holding of a corporate position shall not, by itself, give rise to criminal liability.
- c) **License Suspension or Revocation** — In addition to the penalties above, and only upon a second conviction, the court may order suspension, for a period the court shall fix, of the service provider's license or registration to operate in the Philippines; upon a third or subsequent conviction, the court may order its revocation.

- d) **Foreign Juridical Entities** — Where the offender is a foreign juridical entity without a license to operate in the Philippines, the Cybercrime Court may, upon petition and after the procedure under Section 8, order that its web domain or IP access within Philippine territory be blocked.
- e) **Conspiracy** — A conspiracy to commit any act prohibited under Section 5 shall be punished by the penalty next lower in degree than that prescribed for the consummated offense. A conspiracy exists when two or more persons agree to commit any of the prohibited acts and decide to commit it.
- f) **Proposal to Commit Conspiracy** — A proposal to commit conspiracy under this Act shall be penalized by imprisonment of one (1) year to three (3) years, or a fine of not less than Two Hundred Thousand Pesos (PHP 200,000.00), or both.
- g) **Administrative Fines** — Administrative violations under Section 7 shall be penalized as provided therein, and not under this Section.

SEC. 18. Confidentiality. — All records, proceedings, and reports pertaining to a minor victim, respondent, or witness under this Act shall be kept confidential, consistent with Republic Act No. 9344 and Republic Act No. 7610. The identity of a minor shall not be disclosed to the public in any manner.

SEC. 19. Jurisdiction. — The Regional Trial Courts of the Philippines, specially designated as "Cybercrime Courts," shall have jurisdiction over any violation of this Act. This Act shall also apply to any person or entity that commits a prohibited act outside the geographical boundaries of the Philippines, provided that:

- a) The offense is directed against a minor who is a citizen or resident of the Philippines at the time the offense was committed;
- b) The offense causes or is intended to cause harm, radicalization, or exploitation within the territory of the Philippines; or
- c) The online platform, digital network, or hosting service used in the commission of the offense is accessible to users within Philippine jurisdiction.

SEC. 20. Relation to Other Laws. — This Act shall be construed together with, and shall not be construed to diminish the protections and standards under, Republic Act No. 10175 (Cybercrime Prevention Act of 2012), Republic Act No. 11930 (Anti-OSAEC and Anti-CSAEM Act), Republic Act No. 10627 (Anti-Bullying Act of 2013), Republic Act No. 9344 (Juvenile Justice and Welfare Act of 2006), Republic Act No. 10173 (Data Privacy Act of 2012), and Republic Act No. 7610.

SEC. 21. Appropriations. — The amount necessary for the initial implementation of this Act shall be charged against the current year's appropriations of the DICT, DOJ, PNP, DepEd, DSWD, and DOH. Thereafter, such sums as may be necessary shall be included in the annual General Appropriations Act.

SEC. 22. Implementing Rules and Regulations. — Within sixty (60) days from the effectivity of this Act, the DICT, in coordination with the National Telecommunications Commission, the DOJ, the PNP, DepEd, DSWD, DOH, and the National Privacy Commission, shall promulgate the rules and regulations necessary for its effective implementation.

SEC. 23. Periodic Review. — The Council shall, within three (3) years from the effectivity of this Act and every three (3) years thereafter, submit to Congress a review of the implementation and impact of this Act, including its effect on lawful expression and access to information, together with any recommended amendments.

SEC. 24. Separability Clause. — If any provision of this Act is declared unconstitutional or invalid, the remaining provisions not affected shall continue to be in full force and effect.

SEC. 25. Repealing Clause. — All laws, decrees, executive orders, rules, and regulations, or parts thereof, inconsistent with this Act are hereby repealed, amended, or modified accordingly; provided, that this repealing clause shall not be construed to repeal or amend Republic Act No. 10175, Republic Act No. 11930, Republic Act No. 9344, Republic Act No. 10173, or Republic Act No. 7610, which shall be read together with this Act.

SEC. 26. Effectivity. — This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in at least two (2) newspapers of general circulation.

Approved,