

**Republic of the Philippines
HOUSE OF REPRESENTATIVES**

Quezon City

**TWENTIETH CONGRESS
Second Regular Session**

House Bill No. 10574



Introduced by Representative Richard I. Gomez, DPA

EXPLANATORY NOTE

Article II, Section 13 of the 1987 Constitution mandates the State to promote and protect the physical, moral, spiritual, intellectual, and social well-being of the youth. As children increasingly communicate, learn, play, and participate in public life through digital services, this constitutional duty must extend to the online environment.

Social media platforms, interactive gaming services, and other networked digital environments offer substantial educational, creative, and social benefits. At the same time, their design and operation may expose children to online sexual exploitation, online grooming (whereby offenders gain a child's trust through digital communications for the purpose of sexual exploitation, abuse, coercion, or other harm), cyberbullying, privacy violations, harmful content, commercial profiling, contact with unknown adults, and features that encourage excessive or compulsive engagement.

Recent events have further intensified public concern over the possible influence of violent digital content on minors. In the tragic school shooting in Tacloban City, Leyte, authorities confirmed that one of the two (2) suspects had previously engaged with a violent video game identified as GoreBox. According to the Police Regional Office Eastern Visayas (PRO 8), in a statement reported on June 23, 2026, the 14-year-old suspect was the one who played the game prior to the incident. He further described the game as involving shooting mechanics and firearms-based gameplay, and characterized its content as relatively violent.

Existing laws punish many forms of online abuse and exploitation but mostly after they occur. A complementary preventive framework is therefore very much needed, and one that establishes age-appropriate access, requires providers to assess and reduce foreseeable risks to children, strengthens parental and educational support, and provides effective but proportionate government oversight.

This measure establishes sixteen (16) years as the general minimum age for independently maintaining an account on social media and interactive gaming services, specifically determined in the resulting IRR. It permits only the operation of narrowly defined age-appropriate access arrangements that comply with strict child-safety, privacy, and parental-control requirements. It also provides enhanced protections for all child users, including those aged sixteen (16) and seventeen (17).

On the international front, there is a clear trend toward strengthening protections for minors in digital spaces by means of age-based restrictions. In Australia, the Online Safety Amendment (Social Media Minimum Age Act 2024) took effect in December 2025, setting a minimum age of sixteen (16) for access to specified social media platforms. Indonesia has also begun implementing restrictions barring users under sixteen (16) from major social media and online platforms, becoming one of the first countries in the region to adopt such a framework.

In Europe, countries such as France, Spain, Greece, and Slovenia have introduced or are advancing proposals to establish minimum age thresholds ranging from fifteen (15) to sixteen (16) years, indicating ongoing policy efforts to limit early exposure to online risks. In Germany and Denmark, similar measures remain under legislative discussion or policy consideration, while Malaysia has likewise expressed regulatory intent toward adopting a minimum age requirement for social media access.

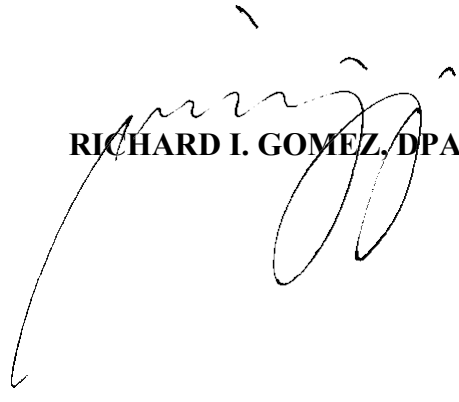
Our national statistical data further shows the urgency of such regulatory action. Based on the 2024 National Information and Communications Technology Household Survey conducted by the Philippine Statistics Authority in partnership with the Department of Information and Communications Technology, approximately two-thirds ($\frac{2}{3}$) of children aged ten (10) to sixteen (16) have accessed the internet within a recent three-month period.

This bill similarly recognizes that age checks may themselves create privacy risks, hence it adopts the principle of age assurance rather than prescribing a rigid list of identification or biometric technologies. Any method used must be necessary, proportionate, accessible, data-minimizing, and subject to standards developed with the National Privacy Commission. The commercial use, profiling, or unnecessary retention of age-assurance information is expressly prohibited.

The bill further requires child-safety-by-design measures, accessible reporting systems, reasonable controls against circumvention, independent risk assessments, and special protections relating to direct messaging, location sharing, targeted advertising, recommender systems, livestreaming, and other high-risk features.

To ensure enforceability, the measure establishes graduated penalties and clarifies the application of the law to foreign providers offering services in the Philippines.

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



RICHARD I. GOMEZ, DPA

**Republic of the Philippines
HOUSE OF REPRESENTATIVES**

Quezon City

**TWENTIETH CONGRESS
Second Regular Session**

House Bill No. 10574

Introduced by Representative Richard I. Gomez, DPA

**AN ACT
ESTABLISHING A CHILD ONLINE SAFETY AND AGE-APPROPRIATE DIGITAL
ACCESS FRAMEWORK, PRESCRIBING OBLIGATIONS FOR DIGITAL PLATFORM
PROVIDERS, STRENGTHENING PRIVACY, PARENTAL SUPPORT, DIGITAL
CITIZENSHIP, AND DUE PROCESS, PROVIDING PENALTIES, AND FOR OTHER
PURPOSES**

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 “*Child Online Protection and Social Media Regulation Act.*”

SEC. 2. *Declaration of Policy.* — It is the policy of the State to protect children from online abuse, exploitation, harmful contact, privacy violations, age-inappropriate content, and digital practices prejudicial to their development, while recognizing the educational, communicative, creative, and social benefits of digital technologies.

Towards this end, the State shall establish an age-appropriate and risk-based framework for children’s access to covered digital services; require providers to adopt child-safety-by-design and privacy-protective measures; strengthen parental, educational, and community support; and ensure that regulation is proportionate, technologically neutral, and consistent with due process and the right to privacy.

SEC. 3. *Objectives.* — This Act shall:

- a. establish a general minimum age for independently maintaining accounts on covered services;

- b. require reasonable and proportionate measures to prevent and reduce foreseeable risks to children;
- c. promote privacy-protective, accessible, and non-discriminatory age assurance;
- d. provide enhanced safeguards for child users, including those aged sixteen (16) and seventeen (17);
- e. strengthen parental controls, reporting mechanisms, and digital citizenship education; and
- f. provide fair, effective, and narrowly tailored enforcement against domestic and foreign providers.

SEC. 4. *Definition of Terms.* — For purposes of this Act:

- a. “**Age Assurance**” refers to a process or combination of measures used to establish, estimate, or confirm whether a user meets an age threshold, without collecting more personal information than is reasonably necessary;
- b. “**Age-Appropriate Service Mode**” refers to a version, setting, or experience of a Covered Digital Service designed for users below sixteen (16) years of age and approved under standards issued pursuant to this Act;
- c. “**Child or Minor**” refers to a person below eighteen (18) years of age;
- d. “**Child-Safety-by-Design**” refers to the integration of children’s safety, privacy, developmental needs, and best interests into the design, operation, testing, and modification of a digital service;
- e. “**Covered Digital Service**” refers to an internet-based service, application, platform, game, or interactive digital environment that has, as a substantial feature, social networking, public or semi-public user-generated content, livestreaming, direct communication with non-household users, persistent multiplayer social interaction, or algorithmic content recommendation, and that is reasonably likely to be accessed by children in the Philippines;
- f. “**Digital Platform Provider**” or “**Provider**” refers to a person or entity that owns, operates, controls, or makes a Covered Digital Service available to users in the Philippines;
- g. “**Grooming**” refers to a deliberate course of conduct carried out through a Covered Digital Service or other electronic means to gain a child’s trust, confidence, dependency, or compliance, or to manipulate or desensitize the child, for the purpose of facilitating sexual exploitation or abuse, coercion, trafficking, extortion, recruitment into unlawful activity, an in-person meeting for a harmful purpose, or any other form of harm;
- h. “**High-Risk Feature**” refers to a design or functionality that creates a material and reasonably foreseeable risk to children, including unrestricted contact by unknown adults, precise location sharing, public default settings, targeted advertising based on profiling,

livestreaming, manipulative recommender systems, autoplay, infinite scrolling, or excessive notifications;

i. **“Independent Account”** refers to an account maintained by a user without an approved Age-Appropriate Service Mode or other protection specifically authorized under this Act and its implementing rules;

j. **“Personal Data”** has the meaning assigned under Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012; and

k. **“Regulatory Authority”** refers to the Department of Information and Communications Technology, without prejudice to the lawful mandates of the National Privacy Commission, National Telecommunications Commission, Council for the Welfare of Children, and other competent agencies.

SEC. 5. *Scope and Excluded Services.* — This Act shall apply to all Covered Digital Services offered, directed, or made substantially available to users in the Philippines, regardless of the Provider’s place of incorporation or principal office.

Exempted from the scope are Services whose primary purpose is formal education, health care, emergency assistance, government service delivery, employment, enterprise collaboration, or private family communication shall not be covered solely by reason of incidental communication functions, provided that they do not substantially operate as open social networks or expose children to comparable risks.

Furthermore, purely offline games, services that do not permit user-to-user communication or user-generated content, and access to publicly available information that does not require an account shall not be restricted under the minimum-age rule. The DICT, in consultation with the Council for the Welfare of Children and the National Privacy Commission, shall issue and periodically update functional criteria for coverage and exclusion.

SEC. 6. *Minimum Age and Age-Appropriate Access.* — A person below sixteen (16) years of age shall not independently create, register, or maintain an account on a Covered Digital Service.

A Provider may offer an Age-Appropriate Service Mode to a person below sixteen (16) years of age only when the mode complies with standards issued under this Act, uses the highest privacy and safety settings by default, restricts High-Risk Features, and obtains verifiable parental or guardian authorization when required by the Implementing Rules and Regulations (IRR) of this Act.

Nothing in this section shall prevent a child from accessing public-interest, educational, health, emergency, or government information that is available without maintaining an account, or from using an excluded service under Section 5.

SEC. 7. *Standards for Age Assurance.* — A Provider shall use reasonable, proportionate, effective, and regularly reviewed Age Assurance measures appropriate to the nature, scale, and risk of the service. No Provider shall rely solely on self-declared age when the service presents a material risk to children.

Age Assurance standards shall be technologically neutral and shall prioritize methods that disclose only whether the applicable age threshold has been met. Such methods shall be accurate enough for their purpose, accessible to persons without standard identification, non-discriminatory, independently auditable, and accompanied by a reasonable process for correction and appeal.

The DICT shall issue Age Assurance standards in consultation with the National Privacy Commission, Council for the Welfare of Children, Philippine Statistics Authority, child-rights and privacy experts, affected industries, parents, and young persons.

SEC. 8. *Privacy and Data Protection Safeguards.* — The collection, processing, storage, disclosure, and deletion of Personal Data under this Act shall comply with Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, and the principles of necessity, proportionality, transparency, purpose limitation, data minimization, security, and limited retention.

A Provider or third-party Age Assurance service shall not:

- a. retain a copy of an identification document or raw biometric information longer than strictly necessary for verification, unless retention is expressly required by law;
- b. use Age Assurance information for advertising, commercial profiling, recommendation systems, or any purpose unrelated to compliance and child safety;
- c. sell, disclose, or share Age Assurance information except as necessary to perform the verification, comply with law, or respond to a lawful order;
- d. require biometric processing when a less intrusive and reasonably effective method is available; or
- e. deny access solely because a person lacks a particular identification document when a reasonable alternative method can be provided.

Any security incident involving Age Assurance information shall be reported and addressed in accordance with the Data Privacy Act and applicable rules of the National Privacy Commission.

SEC. 9. *General Duties of Providers.* — A Provider shall:

- a. conduct and document periodic child-risk assessments appropriate to the nature, scale, and reach of the service;
- b. adopt reasonable, proportionate, effective, and regularly reviewed measures to detect and prevent underage circumvention;

- c. provide accessible parental controls and age-appropriate account settings;
- d. maintain prompt, child-friendly, and accessible reporting, complaint, and appeal mechanisms;
- e. act expeditiously on credible reports of grooming, exploitation, threats, or other serious risks, consistent with due process and existing law;
- f. provide clear notices, in language understandable to children and parents, regarding data practices, safety tools, and material risks;
- g. retain records reasonably necessary to demonstrate compliance, subject to privacy and security safeguards; and
- h. submit annual transparency and compliance reports to the DICT in the form prescribed by the implementing rules.

SEC. 10. *Child-Safety-by-Design.* — Providers shall assess and mitigate the risks that High-Risk Features may present to children. The DICT shall issue proportionate standards based on the nature, size, capabilities, and risk profile of the service.

Such standards shall address, where applicable, private settings by default; contact by unknown adults; direct messaging; precise location sharing; livestreaming; targeted advertising; commercial profiling; recommender systems; autoplay; infinite scrolling; nighttime and excessive notifications; in-app purchases; and tools that facilitate grooming, coercion, or evasion of parental controls.

No standard under this section shall require the monitoring of all private communications or the indiscriminate collection of identity information.

SEC. 11. *Enhanced Protection for Users Aged Sixteen and Seventeen.* — A Provider shall apply heightened privacy, safety, and transparency protections to users aged sixteen (16) and seventeen (17), including private settings by default, restrictions on targeted advertising based on sensitive profiling, safeguards against unsolicited contact by unknown adults, and accessible controls over recommendation and notification features.

SEC. 12. *Parental Controls, Complaints, and Child Participation.* — Providers shall make parental controls and safety information readily accessible without requiring the disclosure of unnecessary personal data. Complaint and appeal procedures shall be understandable to children and shall not expose a reporting child to retaliation or unnecessary publicity.

In developing standards and reviewing implementation, the DICT and the Council for the Welfare of Children shall provide appropriate mechanisms for consultation with parents, educators, child-rights organizations, and young persons, consistent with the evolving capacities and best interests of the child.

SEC. 13. *Responsibilities of Parents and Guardians.* — Parents and legal guardians shall exercise reasonable supervision and promote responsible digital behavior, taking into account the age, maturity, needs, and best interests of the child. Nothing in this Act shall impose criminal liability upon a parent or guardian solely because a child obtained unauthorized access to a Covered Digital Service.

SEC. 14. *Digital Citizenship Education.* — The Department of Education shall integrate age-appropriate instruction on digital citizenship, privacy, cybersecurity, media and information literacy, online ethics, reporting of abuse, and digital well-being into the basic education curriculum.

The Commission on Higher Education and the Technical Education and Skills Development Authority shall, within their respective mandates, promote corresponding programs and guidance for learners, educators, and institutions. Government agencies shall develop accessible information materials for parents and communities.

SEC. 15. *Lead and Coordinating Agencies.* — The DICT shall serve as the primary coordinating and implementing agency for this Act, without diminishing the statutory authority of other agencies. It shall:

- a. issue and periodically review technical and compliance standards;
- b. monitor compliance and receive complaints;
- c. coordinate child-risk, privacy, telecommunications, education, and enforcement matters with the proper agencies;
- d. maintain a public registry of final compliance orders and accredited third-party Age Assurance providers, subject to lawful confidentiality requirements; and
- e. conduct public education and submit reports to Congress.

The DICT shall coordinate with the National Privacy Commission (NPC), National Telecommunications Commission (NTC), Department of Education (DepED), Commission on Higher Education (CHED), Department of Social Welfare and Development (DSWD), Department of Justice (DOJ), Philippine National Police (PNP), National Bureau of Investigation (NBI), and Council for the Welfare of Children (CWC), consistent with their respective mandates.

SEC. 16. *Foreign Providers and Local Representation.* — A foreign Provider that offers a Covered Digital Service to users in the Philippines and meets the user, revenue, or risk thresholds prescribed in the Implementing Rules and Regulations (IRR), according to Sec. 21 of this Act, shall designate a local representative authorized to receive notices, orders, and legal process.

The IRR shall likewise establish objective thresholds and reasonable compliance requirements, taking into account the number of Philippine users, accessibility to children, local revenue, and the nature and severity of foreseeable risks.

SEC. 17. *Compliance Assessments and Independent Audits.* — The DICT may require a Provider presenting significant or systemic risks to children to submit a child-risk assessment or undergo an independent audit by a qualified entity. Any requirement shall be proportionate, protect trade secrets and Personal Data, avoid unnecessary duplication, and allow the Provider to respond to material findings.

SEC. 18. *Penalties.* — After notice and hearing, a Provider or third-party Age Assurance service that violates this Act or its implementing rules may be subject to the following penalties:

- a. for a first violation, a fine of not less than One Million Pesos (P1,000,000.00) but not exceeding Five Million Pesos (P5,000,000.00);
- b. for a second violation, a fine of not less than Five Million Pesos (P5,000,000.00) but not exceeding Ten Million Pesos (P10,000,000.00);
- c. for a subsequent, repeated, or willful violation, a fine of not less than Ten Million Pesos (P10,000,000.00) but not exceeding Thirty Million Pesos (P30,000,000.00); and
- d. for failure to comply with a final lawful order after a prescribed period, a Provider or third-party Age Assurance service shall be served a cease and desist order from the relevant court based on the IRR.

Misuse of Personal Data shall be referred to the NPC and shall be subject to the Data Privacy Act and other applicable laws. These administrative penalties are without prejudice to civil or criminal liability under existing law.

SEC. 19. *Congressional Oversight and Periodic Review.* — The House Committees on Information and Communications Technology, and Welfare of Children and the Senate Committee on Women, Children, Family Relations and Gender Equality shall exercise oversight over the implementation of this Act.

Within three (3) years from effectivity, and every three (3) years thereafter, the DICT, in consultation with the relevant agencies and stakeholders, shall submit to Congress an evaluation of the law's effectiveness, effects on children's rights and access to beneficial services, privacy impacts, enforcement outcomes, technological developments, and recommended amendments.

SEC. 20. *Appropriations.* — The amount necessary for the initial implementation of this Act shall be charged against the current appropriations of the concerned agencies. Thereafter, the amounts necessary for its continued implementation shall be included in the annual General Appropriations Act, subject to existing budgeting, accounting, and auditing laws.

SEC. 21. *Implementing Rules and Regulations.* — Within one hundred eighty (180) days from effectivity, the DICT, in consultation with the NPC, NTC, DepEd, CHED, DSWD, DOJ, CWC, child-rights and privacy experts, parents, young persons, and representatives of affected industries, shall promulgate the rules necessary to implement this Act.

The rules shall include objective functional criteria for covered services; standards for Age-Appropriate Service Modes and Age Assurance; child-safety-by-design requirements; risk-based thresholds for foreign Providers; audit and reporting standards; complaint and appeal procedures; and reasonable compliance periods.

SEC. 22. *Transition Period.* — Providers shall be given twelve (12) months from the effectivity of the implementing rules to achieve full compliance, unless a shorter period is necessary to address a clear and imminent risk of grave harm. The DICT may establish phased requirements based on service size, technical capacity, and risk to children.

SEC. 23. *Separability Clause.* — If any provision of this Act is declared unconstitutional or invalid, the remaining provisions not affected thereby shall remain in full force and effect.

SEC. 24. *Repealing Clause.* — All laws, decrees, executive orders, rules and regulations inconsistent with this Act are hereby repealed, amended, or modified accordingly.

SEC. 25. *Effectivity.* — This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in at least one (1) newspaper of general circulation.

Approved,