

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. **11464**



Introduced by Representative ELMER V. CATULPOS
(I-Tahanan Party-List)

EXPLANATORY NOTE

Alas-nuwebe kuwarenta ng gabi sa isang maliit na bahay sa Tagum City. Kumakalansing ang electric fan sa bawat pihit. Nauupos ang katol sa platito. Sa ilalim ng manipis na kumot, ang tanging liwanag sa silid ay ang teleponong nakatutok sa mukha ng isang batang babae, labing-isang taong gulang, na tatawagin nating Mika.

Naka-night shift ang kaniyang ina sa isang ospital sa Riyadh. Namamasada ang kaniyang ama hanggang hatinggabi. Ang tanging gising sa bahay ay ang kaniyang Ate, disinuwebe anyos, nagrerepaso para sa eksamen sa kabilang silid.

Sa screen, isang manlalarong siyam na araw pa lamang niyang nakilala ang nagpadala ng apat na raang play money ng laro. Pagkatapos, isang mensahe: "ur my best friend here. add me on another app so we can really talk. dont tell ur ate ok?"

Si Mika ay tauhang binuo mula sa mga totohanang kaso. Walang hakbang sa tagpong ito na inimbento. Ang regalo, ang pagkakaibigang binuo sa loob ng ilang araw, ang paanyayang lumipat sa pribadong channel, ang bilin na maglihim — ito ang pattern na naitala ng United States Federal Bureau of Investigation, ng ating PNP Anti-Cybercrime Group, at ng mga mananaliksik sa proteksiyon ng bata.

What most parents do not know

No law of the Republic says who may talk to a child inside a game.

Whether a stranger can find Mika, speak to her, send her gifts, or invite her elsewhere is decided today by the terms of service of a foreign company — rules written, and rewritten, in a boardroom she will never see. Many games are no longer only games. They are social places, where chat, voice, friend requests, searchable profiles, gifts, and recommendations combine to make contact easier than any parent realizes.

The strongest of the companies' own rules is the age check. Within days of its worldwide launch, age-verified accounts were being offered for sale online for about the price of a cup of coffee. The door that matters is therefore not the door into the game. It is the door between a child and a stranger, once both are inside.

The numbers, after the child

- (a) The FBI classifies the network known as “764” as nihilistic violent extremism. Its public warnings describe first contact on gaming platforms popular with children, followed by movement of the victim to private channels.
- (b) The PNP Anti-Cybercrime Group has reported *seventeen (17) rescue operations involving twenty-four (24) minor* connected to online grooming.
- (c) The Institute for Strategic Dialogue has linked to an online subculture that glorifies mass killers, whose members build game maps that re-enact real massacres.
- (d) Our country has suffered three school shootings in eighty-eight days: Tacloban City on 22 June, Zamboanga City on 18 August, and Banga, South Cotabato on 18 September 2026. The investigations will establish what led to each, and this Representation will not run ahead of them. This bill does not depend on their answer. It rests on one fact that is not in dispute: the door was open.
- (e) In September 2025, one of the world's largest children's gaming platforms suspended in-game chat across the Arabic-speaking Middle East after discussions with regulators there; two countries restored access on condition that chat stay off. What other governments obtained by negotiation, Filipino children should hold by law.

Gratitude, and the gap

In his State of the Nation Address last July, the President said of the violence that reached our schools:

“Kailangang mamulat ang buong lipunan at akuin ang responsibilidad.”

Much has been done in answer. The Department of Information and Communications Technology and the Cybercrime Investigation and Coordinating Center placed a major platform under probation and secured a direct line for our investigators. The Senate advanced the measure now known as the Sagip Bata Act. This House, under the Speaker and the Majority Leader, and through the Committee on Welfare of Children and its Technical Working Group, moved the Children's Social Media and Online Gaming Safety Act. A separate pending House measure on video-game communications proposes privacy by default and limits on adult contact with minors.

This bill competes with none of them. Those measures decide who may hold an account, what platforms owe the State, and how offenders are punished. This bill answers the one

question they leave open: once a child is lawfully inside a game, who may find her, and who may speak to her?

Ang kalaban ay hindi ang laro

Isang henerasyon ng Pilipino ang lumaki sa mga laro, pati sa mararahas na laro, at naging nars, marino, inhinyero, at magulang. Ang kalaban ay hindi ang laro. Hindi ang gamer. Hindi ang inang naka-night shift sa ibang bansa, hindi ang amang hindi nakaaalam kung ano ang server, at hindi ang batang hindi agad nakilala ang panlilinlang. Ang kalaban ay isang bukas na pinto — isang default setting na nagpapahintulot sa sinumang stranger na hanapin at lapitan ang sinumang bata.

Bawat gabing nakabukas ang pintong iyon ay gabing may kumakatok. At ang proteksiyong ibinigay ng isang kompanya sa pamamagitan ng polisiya ay maaaring bawiin ng kompanyang iyon sa pamamagitan ng polisiya. Ang kaligtasan ng bata ay hindi dapat nakasalalay sa quarterly earnings call ng isang dayuhang korporasyon.

One principle: sarado hanggang buksan

The architecture of this bill fits in one sentence: every channel between a child and another player is closed until a guardian opens it — one person at a time, never to strangers as a class. From that principle follow five pillars.

- (1) **Closed and hidden by default.** No voice, text, file, link, or gift passes between a child and any account her guardian has not approved. A child cannot be searched, recommended, followed, or located by strangers. A request to connect goes to the guardian, not to the child. On platforms built for children, voice features are switched off in the Philippines altogether.
- (2) **The Kuya-Ate Guardian.** The law has always assumed that the parent holds the controls. In the Filipino home, the one who understands the game is often the Ate in the next room. This bill lets a parent lawfully hand her the keys — through a console that works on a shared phone, on weak signal, and by text message.
- (3) **Cut the bridge.** An invitation to a child to leave the game for a private channel is blocked. The consequence falls on the sender — never on the child. Selling or buying age-verified accounts becomes a crime.
- (4) **No massacre games.** Interactive re-enactments that place a player in the role of the perpetrator of a real mass attack are removed.
- (5) **Teeth.** A platform that fails may be ordered, step by step and with due process, to switch off voice, then all chat, then its sales in the Philippines, then access. Fines scale with Philippine revenue. A child who is harmed because the door was left open may sue.

Sa araw na gumana ang batas na ito

Hindi na kailangang maging unang depensa ng kaniyang sarili ang isang batang labing-isang taong gulang. Maglalaro si Mika, tatawa, at matutulog. Ang mensaheng iyon ay hindi kailanman makararating sa kaniyang screen. At sa telepono ng kaniyang Ate sa kabilang silid, isang alerto: may account na tinangkang ilipat ang iyong kapatid sa ibang app. Hinarang.

What this bill does not do

It does not ban any game. It does not touch conversations between adults on general and competitive gaming platforms; the team communications of Filipino esports are left alone. It does not authorize anyone to read the private messages of adults. It does not score, label, or profile any child. It does not ask any family to surrender more personal data than safety requires. And it does not punish a child, or a household, for being targeted.

Disclosure

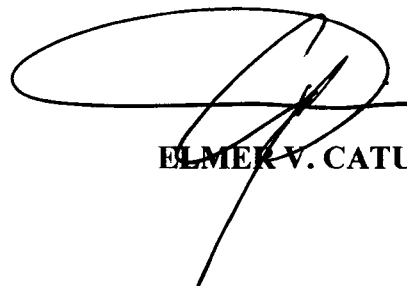
This Representation discloses that neither he nor any enterprise he founded holds an interest in any gaming or technology platform covered by this measure. He is the founder of a radio network whose stations take the calls of parents every day, and he is a grandfather. He files this bill as a witness to those calls.

Hindi pa ito batas. Kapag naipasa, ito ang pangakong maaaring bigkasin ng bawat magulang, bawat Kuya, at bawat Ate:

“Walang stranger na makakausap ng batang Pilipino sa laro.”

“Hindi ang laro ang kalaban. Ang kalaban ay ang stranger sa loob ng laro.”

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



ELMER V. CATULPOS

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 11464

Introduced by Representative ELMER V. CATULPOS
(I Tahanan Party-list)

AN ACT PROTECTING CHILDREN FROM CONTACT AND DISCOVERY BY STRANGERS IN ONLINE GAMES, REQUIRING THAT THE COMMUNICATION AND DISCOVERY FEATURES OF ONLINE GAMING PLATFORMS BE CLOSED BY DEFAULT FOR CHILDREN, ESTABLISHING THE KUYA-ATE GUARDIAN SYSTEM, PROHIBITING THE SOLICITATION OF CHILDREN TO MOVE TO PRIVATE CHANNELS, THE TRAFFICKING OF AGE-VERIFIED ACCOUNTS, AND THE HOSTING OF MASS-ATTACK RECREATIONS, PROVIDING FOR PLATFORM ACCOUNTABILITY, CIVIL LIABILITY, AND PENALTIES, APPROPRIATING FUNDS THEREFOR, AND FOR OTHER PURPOSES

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

ARTICLE I
GENERAL PROVISIONS

SEC. 1. Short Title. – This Act shall be known as the “**Bantay-Laro Act**” or the “Children’s Online Game Communication Safety Act of 2026.”

SEC. 2. Declaration of Policy. – The State recognizes the vital role of the youth in nation-building and shall promote and protect their physical, moral, spiritual, intellectual, and social well-being. It shall defend the right of children to special protection from all forms of neglect, abuse, cruelty, exploitation, and other conditions prejudicial to their development, and shall support the natural and primary right and duty of parents in the rearing of the youth. Toward these ends, it is the policy of the State that:

- (a) Play is a right of the child. Online games are not the enemy of the State, and nothing in this Act shall be construed to prohibit any game;

- (b) No stranger shall be permitted by a covered platform to discover or communicate with a child account through a covered platform, except through an approved connection affirmatively authorized in accordance with this Act.
- (c) The burden of protection shall rest on the platforms that profit from children's play and on the persons who prey on children — never on the child who is targeted, nor on the household that lacks the means to watch over her every hour;
- (d) The law shall recognize the Filipino family as it is, including the households of overseas Filipino workers, households that share one device, and the older brothers and sisters who stand in daily care of the young;
- (e) No child or family shall be required to surrender more personal data than is necessary for protection; and
- (f) Protection shall be achieved by the means least intrusive on the lawful speech and privacy of adults and on the privacy, dignity, and evolving capacities of children.

SEC. 3. Definition of Terms. – As used in this Act, the following terms shall be defined as follows:

- (a) **Age-verified account** refers to an account on an online gaming platform that has passed any age assurance, identity verification, or guardian-linking process of that platform;
- (b) **Approved connection** refers to an account that a Guardian or Kuya-Ate Guardian has affirmatively approved, through the Guardian Console, to communicate with a specific child account;
- (c) **Child** refers to a person below eighteen (18) years of age;
- (d) **Child account** refers to an account held or used by a child, including any account treated as a child account under Section 10;
- (e) **Child-dominant platform** refers to an online gaming platform (1) that is directed to children, as shown by its design, content, marketing, or age ratings; or (2) in which child accounts comprise at least *thirty percent (30%)* of monthly active accounts in the Philippines, as determined by the Office under Section 21;
- (f) **Communication feature** refers to any function of an online gaming platform that allows one account to convey to another any free-form text, voice, video, image, file, hyperlink, contact detail, or gift, whether inside a game, in a lobby, in a group or party, or by direct message. It excludes preset expressions drawn from a fixed list that cannot carry free-form content;
- (g) **Covered platform** refers to any child-dominant platform, and to any other online gaming platform with at least *one hundred thousand (100,000)* monthly active accounts in the Philippines;
- (h) **Discovery feature** refers to any function by which an account may search for, find, view the profile of, follow, invite, send a connection request to, be recommended to, or be matched by location with another account;
- (i) **General platform** refers to a covered platform that is not a child-dominant platform;

- (j) **Gift** refers to any transfer of virtual currency, virtual item, subscription, code, or other thing of value from one account to another;
- (k) **Guardian** refers to a parent, or a person exercising parental authority or legal custody over a child under the Family Code and other laws, whose identity and relationship have been verified under Section 11;
- (l) **Guardian Console** refers to the free tool that every covered platform must provide under Section 13;
- (m) **Kuya-Ate Guardian** refers to a an trusted adult designated by a Guardian for limited protective functions under Section 12 and is not a parent, legal guardian, or holder of parental authority;
- (n) **Mass-attack recreation** refers to an interactive game, experience, map, or simulation that places the user in the role of the perpetrator of an actual attack that killed or was intended to kill multiple persons in a school or other public place, or that materially rewards, encourages, or glorifies the perpetrator's conduct. It does not include bona fide news reporting, historical analysis, education, research, memorialization, documentary treatment, or works in which the user is not placed in the perpetrator's role;
- (o) **Monetization feature** refers to any function by which a covered platform receives payment from or on behalf of accounts located in the Philippines, including the sale of virtual currency, virtual items, and subscriptions;
- (p) **Office** refers to the office designated under Section 27 to administer this Act;
- (q) **Off-platform solicitation** refers to any message, utterance, image, code, or other communication that invites, instructs, or induces a child to communicate through another application, service, account, or channel, to disclose a contact detail for that purpose, or to keep a communication secret from a Guardian;
- (r) **Online gaming platform** refers to any digital service accessible in the Philippines whose primary purpose is to allow users to play, create, or host interactive games, and which offers any communication feature or discovery feature between users, regardless of the device used;
- (s) **Stranger** refers, in relation to a child account, to any account that is not an approved connection of that child account; and
- (t) **Voice feature** refers to any communication feature that transmits live or recorded speech between accounts.

SEC. 4. Coverage. – This Act applies to every covered platform, wherever established, in respect of accounts located in or accessed from the Philippines. A platform may not avoid coverage by the absence of a Philippine office, server, or registration.

A covered platform that is a micro, small, or medium enterprise under Republic Act No. 9501 shall be entitled to technical assistance from the Office and to the additional compliance period in Section 30(c). The implementing rules shall provide a simplified compliance pathway for such enterprises, which shall not reduce any protection of the child under Article II.

ARTICLE II

CLOSED AND HIDDEN BY DEFAULT

SEC. 5. The Closed-by-Default Rule. – To protect children from unsolicited, inappropriate, or potentially harmful communications and interactions on digital platforms, a covered platform shall adopt a closed-by-default approach for child accounts. Accordingly, communication and interaction features involving a child account shall, by default, be restricted to persons or accounts that have been expressly approved in accordance with this Act and the platform’s applicable child-safety mechanisms.

- (a) A covered platform shall disable, by default, communication between a child account and an account that is not an approved connection.
- (b) A covered platform shall disable, by default, discovery of a child account by an account that is not an approved connection. A child account shall not be searchable, recommended, followed, invited, or matched by location with such account. A connection request involving a child account shall be delivered to the Guardian Console and not directly to the child account.
- (c) A communication or discovery feature may be opened for a child account only in respect of a specific approved connection. No setting, consent, or act — whether of the child, of a Guardian, or of the platform — shall open a child account to strangers as a class. No platform may treat a stranger as an approved connection on the basis of its own age-matching, friend-suggestion, or similar process.
- (d) The child shall remain free to play. No child shall be disadvantaged in gameplay, progression, access to essential game functions, or pricing by reason of the protections of this Article.
- (e) Every covered platform shall give the child a notice, suited to a child’s understanding, explaining these protections and how to ask a Guardian or Kuya-Ate Guardian for help.

SEC. 6. Voice Features. – To reduce the risk of unsolicited, inappropriate, or potentially harmful real-time interactions involving children, voice communication features shall be subject to heightened safeguards on child-dominant platforms. Voice functionality, by its nature, may facilitate direct and immediate interaction between users and may expose children to communications that are difficult to monitor or moderate. Accordingly, the following safeguards shall apply:

- (a) On a child-dominant platform, all voice features shall be disabled for all accounts located in or accessed from the Philippines.
- (b) On a general platform, voice features shall be disabled for every child account, except between a child account and an approved connection.
- (c) On any covered platform, no voice feature shall operate between a child account and an account held by an adult, unless that adult is the Guardian or a Kuya-Ate Guardian of the child.
- (d) Nothing in this Section restricts voice features between adults on a general platform.

- (e) This prohibition shall not apply to a voice communication initiated by a platform employee or authorized service provider solely for customer support, safety response, accessibility, or emergency assistance, provided that the communication is logged, limited to the stated purpose, and subject to applicable privacy safeguards.

SEC. 7. Files, Links, and Gifts. – A covered platform shall not permit an account that is not an approved connection to transmit to a child account any image, video, file, hyperlink, contact detail, or other user-generated content.

A covered platform shall not permit such account to send a gift to a child account. A blocked gift shall be returned or securely held and disposed of in accordance with the platform’s published child-safety policy. The attempt shall be recorded as an alert event under Section 14.

SEC. 8. Identity and Location of the Child. – No covered platform shall publicly display, or make available to a stranger, the real name, age, school, address, location, contact information, image, or voice of a child. Precise location sharing and location-based matching shall be disabled for every child account.

SEC. 9. Approved Connections. – To ensure that a child’s online connections are established only with the knowledge and consent of a responsible adult, an approved connection shall require a clear, deliberate, and affirmative act of the Guardian or a duly designated Kuya-Ate Guardian through the Guardian Console. Approval shall not be presumed, inferred from circumstances, or established solely by the conduct or preference of the child.

- (a) A connection is approved only by an affirmative act of the Guardian or a Kuya-Ate Guardian through the Guardian Console. Silence, inaction, or the act of the child alone is not approval.
- (b) Before approval, the platform shall show the approving person, in plain language, the age band of the requesting account, how long it has existed, and whether it has been sanctioned under Section 16. The platform shall not disclose the person’s age, identity document, address, contact information, or other unnecessary personal data. Sanction information shall be accurate, relevant, and subject to correction and appeal.
- (c) Approval shall be specific to one account, shall explain the foreseeable risk in plain language, and may be withdrawn at any time with immediate effect.

SEC. 10. Accounts of Unassured Age; No Excuse. – Where the age of an account holder cannot be reliably established, uncertainty or the absence of verified age information shall not be used as a basis to circumvent, weaken, or withhold the child-safety protections required under this Act. A covered platform shall adopt reasonable safeguards for accounts

whose age remains unverified or uncertain, consistent with the risk-based protections prescribed herein.

- (a) An account whose holder's age has not been assured in the manner required by applicable law, and any account the platform knows or has reason to believe is held by a child, shall be treated as a child account. No account shall be treated as an adult account solely because age assurance was not completed.
- (b) This Act creates no separate age verification system. It adopts whatever age assurance framework is established by law, and applies the more protective classification where age is unknown.
- (c) The liability of a covered platform under this Act shall not be excused by a child's misstatement of age, by the absence of Guardian consent, or by the use of a trafficked account, where the platform failed to maintain reasonable and effective safeguards against the same.
- (d) The platform shall provide a timely, accessible, and human-reviewed process for correcting an erroneous classification. Pending review, the platform may maintain protective restrictions but shall not suspend the child's access to ordinary gameplay solely because age is unresolved.

ARTICLE III

THE KUYA-ATE GUARDIAN SYSTEM

SEC. 11. Guardian Link. – Every child account on a covered platform shall be linked to the verified account of at least one Guardian. Verification shall use the least intrusive reliable means. No child or Guardian shall be refused a link solely for lack of a national identification record; the implementing rules shall provide alternative pathways.

SEC. 12. Kuya-Ate Guardian. – (a) A Guardian may designate not more than *two (2)* persons as Kuya-Ate Guardians of a child account. A Kuya-Ate Guardian must be at least *eighteen (18) years of age* and must be a relative of the child within the fourth civil degree of consanguinity or affinity, or a member of the same household.

- (b) Designation shall be made only from the verified account of the Guardian, shall require verification of the person designated, and may be revoked by the Guardian at any time with immediate effect.
- (c) A Kuya-Ate Guardian may approve and withdraw connections, receive alerts, and file reports. A Kuya-Ate Guardian may not alter the Guardian link, designate another person, or authorize any purchase.
- (d) Designation is not a transfer, waiver, or substitution of parental authority under the Family Code. A Kuya-Ate Guardian who acts in good faith incurs no civil or criminal liability for the acts of third persons. The duty to protect the child remains with the platform and the Guardian; the Kuya-Ate Guardian is a helper, not a substitute for safe design.

- (e) No person convicted by final judgment of an offense involving sexual abuse, sexual exploitation, trafficking, online sexual exploitation of children, child pornography or CSAEM, or other acts against a child under Republic Act Nos. 7610, 9208, as amended, 9775, 11930, 10175, 9262, the Revised Penal Code, or other applicable laws shall be designated. The implementing rules shall prescribe a lawful and privacy-preserving method for determining disqualification.

SEC. 13. Guardian Console. – Every covered platform shall provide, free of charge, a Guardian Console that:

- (a) is available in Filipino and English and, as the implementing rules may require, in other major Philippine languages and in formats accessible to persons with disabilities;
- (b) works on low-cost devices, on a device shared with the child, and under intermittent or limited connectivity;
- (c) delivers alerts by short message service or other low-data channel; and (d) requires no separate device, no continuous internet access, no purchase, no subscription, no advertisement viewing, and no personal information beyond what verification requires.

SEC. 14. Alerts Based on Events, Not on Profiles. To promote objective and timely child-safety interventions, alerts and protective responses under this Act shall be guided by the following:

- (a) The Guardian Console shall alert the Guardian and every Kuya-Ate Guardian upon any of the following events: (1) a request to become an approved connection; (2) an off-platform solicitation blocked under Section 16; (3) a gift blocked under Section 7; (4) an attempt at contact by an account sanctioned under Section 16; and (5) a report filed by or about the child account.
- (b) No covered platform, and no public authority, shall generate, assign, or disclose any score, label, prediction, or profile of a child's beliefs, tendencies, mental state, or propensity for violence by reason of this Act.
- (c) The content of a child's conversations with approved connections shall not be disclosed through the Guardian Console, except the specific message that triggered an alert.

SEC. 15. No Penalty on the Child or the Household. – (a) No child account shall be suspended, terminated, or restricted in play by reason of the inaction, absence, or inability of a Guardian. Where no Guardian link exists, the communication and discovery features remain closed and the child continues to play; and (b) The Department of Social Welfare and Development, the Department of Education, and the Barangay Councils for the Protection of Children shall assist households that lack a Guardian able to operate the Guardian Console, under the program in Section 28.

ARTICLE IV CUT THE BRIDGE

SEC. 16. Off-Platform Solicitation; Consequences Fall on the Sender. – (a) Every covered platform shall employ reasonable and effective measures, consistent with the state of the art, to detect and block any off-platform solicitation addressed to or receivable by a child account, in any communication feature that remains open under this Act, including voice features where allowed. This duty is limited to communications to and from child accounts on the platform’s own service; it creates no duty or authority to monitor communications between adults, or on any other service.

- (b) No consequence shall be imposed on the child account that received the solicitation.
- (c) The platform shall impose on the sending account: a warning for the first instance; suspension of all communication and discovery features for not less than thirty (30) days for the second; and permanent termination, with reasonable measures against re-registration, for the third, or for any instance accompanied by a gift, a request for secrecy, or contact with more than one child.
- (d) Where the sender is a child, the consequence for a first or second instance shall be an educational notice and an alert to the sender’s Guardian.
- (e) A sanctioned account holder shall have access to a prompt appeal decided by a natural person within seventy-two (72) hours. A covered platform that blocks, sanctions, or reports in good faith under this Act, and maintains such appeal, shall incur no civil or criminal liability therefor.

SEC. 17. Reporting, Preservation, and Emergency Response. To ensure the prompt protection of children and timely action against identified risks, covered platforms shall maintain accessible mechanisms for reporting, preservation of relevant information, escalation, and emergency response, consistent with the child’s best interests and applicable privacy safeguards. The following shall apply: –

- (a) Every covered platform shall provide, within each game and within the Guardian Console, a one-step report function that a child can find and understand, and that routes to the platform and, at the option of the reporter, to the national hotlines designated by the Office. Every report shall be acknowledged, and the reporter given a simple means to block the reported account.
- (b) Where circumstances reasonably indicate grooming, recruitment into violence, or sexual exploitation of a child, the platform shall report the matter to the Office and the appropriate law-enforcement agency without undue delay and, in any event, within twenty-four (24) hours from the time the platform obtains sufficient facts to make the report. The platform shall preserve only the relevant data for the period required by Republic Act No. 11930 and its implementing rules, or for a longer period only upon a lawful preservation order.

- (c) Where there is an imminent danger to the life or safety of a child, the platform shall act immediately and without undue delay on lawful request of a law enforcement agencies. Disclosure of subscriber, traffic, or content data shall remain subject to Republic Act No. 10175, the Rules of Court, and other applicable rules of procedures issued by the Supreme Court.

SEC. 18. Trafficking in Age-Verified Accounts. – It shall be unlawful for any person to sell, buy, rent, lend for consideration, broker, or advertise an age-verified account or a Guardian-linked account, or the credentials thereto.

Every online marketplace, social media service, or classified-advertisement service accessible in the Philippines shall remove a listing prohibited by this Section within twenty-four (24) hours from notice by the Office or by a covered platform.

SEC. 19. Mass-Attack Recreations. – To protect children from the harmful effects of simulated mass-casualty violence, covered platforms shall adopt safeguards against the creation, promotion, or participation in mass-attack recreations. The following shall apply:

- (a) No covered platform shall host, distribute, or make available a mass-attack recreation in violation of this Section. The platform shall take reasonable steps to restrict access or remove access to such mass-attack recreation within twenty-four (24) hours from actual knowledge or notice from the Office.
- (b) This Section does not apply to bona fide news reporting, historical or educational works, memorials, or works that do not place the user in the role of the perpetrator.

ARTICLE V

PLATFORM ACCOUNTABILITY, ENFORCEMENT, AND LIABILITY

SEC. 20. Duties of Presence, Foresight, and Transparency. – Covered platforms shall exercise reasonable diligence, anticipate foreseeable risks, and maintain transparency in implementing the child-safety safeguards required under this Act, and shall observe the following:

- (a) **Resident representative.** Every covered platform shall maintain a representative in the Philippines authorized to receive notices, orders, and legal processes under this Act, who shall also be its agent for service of summons in actions under Section 25. Compliance with a resident-representative or registration requirement under any other law protecting children online shall be deemed compliance with this paragraph.
- (b) **Risk assessment before release.** Before introducing or materially changing any communication, discovery, or monetization feature that may affect child accounts, a covered platform shall conduct and document a child-safety risk assessment, including the risk of radicalization toward violent extremism, and shall furnish it to the Office upon request.

- (c) **Bantay-Laro Compliance Report.** Every six (6) months, every covered platform shall publish a report for the Philippines stating: the number of child accounts; the proportion linked to a Guardian; off-platform solicitations blocked; sanctions imposed under Section 16; reports made under Section 17 and response times to law enforcement; listings and recreations removed; and appeals received and granted.
- (d) **Independent audit.** Every covered platform shall submit to an annual independent audit of its compliance, under standards set by the Office. The Office shall publish the results on a public dashboard, presenting improvement beside achievement, and comparing like platforms with like.

SEC. 21. Classification of Platforms. – The Office shall determine and publish, at least once a year, the list of child-dominant platforms, on the basis of data that covered platforms are hereby required to furnish. A platform shall be given notice and the opportunity to contest its classification before the list takes effect. A platform that fails or refuses to furnish the data shall be presumed child-dominant.

SEC. 21-A. Bantay-Laro Child-Safety Certification. – Every covered platform shall obtain from the Office, within one hundred eighty (180) days from the issuance of the implementing rules, and shall renew every year thereafter, a Bantay-Laro Child-Safety Certification, issued upon a showing, verified by the independent audit under Section 20(d), that the platform complies with Articles II, III, and IV and with Section 20 of this Act.

The Certification is a finding of compliance with the child-safety standards of this Act and nothing more. It is not a license to operate, and it involves no review, classification, or approval of the content of any game or communication. A covered platform may operate while its application is pending. The Office shall act on an application within sixty (60) days from its completion; where it fails to act within that period, the platform shall be deemed certified until the Office decides.

The Office shall publish and maintain a public register of certified platforms, showing for each the date of certification, the results of its most recent audit, and any sanction under this Act. A certified platform may display the Bantay-Laro mark in its application-store listing and in its Guardian Console; no uncertified platform shall display it.

The Office shall, after notice and hearing, revoke the Certification of a covered platform that:

- (1) fails two (2) consecutive annual audits under Section 20(d);
- (2) fails to comply with a final order under Section 22 within sixty (60) days; or
- (3) obtained the Certification by fraud or material misrepresentation. A platform whose Certification has been revoked shall be subject to the measures under Section 22(b);(3) and, upon continued non-compliance for thirty (30) days, Section 22(b); and (4) the National

Telecommunications Commission, internet service providers, application distribution services, and the payment entities named in Section 22(d) shall give effect thereto in the manner provided in that Section. The Certification shall be restored upon a showing of compliance.

Certification standards shall be published, technology-neutral, and limited to the duties imposed by this Act. Certification fees shall not exceed the cost of processing and audit review and shall be waived for covered platforms under Section 4(b).

A Certification, registration, or resident-representative requirement under any other law protecting children online shall, to the extent it covers the same standards, be deemed to satisfy this Section, and the Office shall issue a single certificate for both.

SEC. 22. Feature Suspension Order. – To address serious or continuing risks to child safety, the Office may order the temporary suspension of specified platform features, subject to the safeguards and procedures provided under this Act:

- (a) Where a covered platform has materially or repeatedly failed to comply with Articles II, III, or IV, the Office may, after notice and hearing, order the platform to disable specified features for accounts located in or accessed from the Philippines until compliance is shown.
- (b) The Office shall order the narrowest measure adequate to protect children, in this sequence: (1) voice features; (2) all communication and discovery features; (3) monetization features; and (4) only where the foregoing have failed, access to the platform.
- (c) Where there is clear and imminent danger to children, the Office may issue an interim order under paragraph (b)(1) or (b)(2), effective for not more than thirty (30) days, and shall hear the platform within five (5) days from issuance.
- (d) Upon a final order under paragraph (b)(3), banks, electronic money issuers, payment system operators, and application distribution services shall cease processing payments to the platform from accounts in the Philippines, in the manner prescribed by the Bangko Sentral ng Pilipinas in coordination with the Office.
- (e) The National Telecommunications Commission, internet service providers, and application distribution services shall give effect to a final order under paragraph (b)(4) upon request of the Office.
- (f) A final order of the Office may be appealed to the Court of Appeals under Rule 43 of the Rules of Court. The appeal shall not automatically stay the order unless the Court of Appeals directs otherwise.

SEC. 23. Administrative Fines. – To ensure meaningful compliance with the safeguards established under this Act, the Office shall impose proportionate administrative fines for violations, taking into account the circumstances and impact of each violation.

- (a) Without prejudice to Section 22, the Office may impose, after notice and hearing: for failure to file a report, furnish data, or submit to audit, a fine of ₱100,000 to

₱2,000,000; for violation of Articles II, III, or IV, a fine of ₱2,000,000 to ₱20,000,000; for gross or repeated violation, a fine of ₱20,000,000 to ₱50,000,000, or two percent (2%) of the platform's gross revenue derived from the Philippines in the preceding year, whichever is higher; and for continuing violation, a daily fine of ₱100,000 to ₱1,000,000. In determining the amount, the Office shall consider the nature, gravity, duration, number of affected children, degree of negligence or intent, cooperation, and prior violations.

- (b) Fines shall be immediately executory, without prejudice to appeal.
- (c) No fine under this Act shall be imposed on a child, a Guardian, or a Kuya-Ate Guardian.

SEC. 24. Prohibited Acts and Criminal Penalties. – The following actions shall be considered prohibited and sanction by the following penalties:

- (a) Any person eighteen (18) years of age or older who knowingly uses a materially false representation, a trafficked account, or any other deceptive means to circumvent a protection under Article II for the purpose of initiating or maintaining contact with a child account shall be punished by the penalty of *prision correccional in its medium and maximum periods and a fine of ₱200,000 to ₱1,000,000*. Where the act is accompanied by a gift, a request for secrecy, or an off-platform solicitation, or involves two (2) or more children, the penalty shall be *prision mayor and a fine of ₱1,000,000 to ₱3,000,000*.
- (b) Any person who violates Section 18(a) shall suffer the penalty of *prision correccional in its minimum period and a fine of ₱100,000 to ₱500,000*; if the offense involves ten (10) or more accounts, or the offender knows that the account will be used by an adult to reach children, the penalty next higher in degree shall be imposed.
- (c) Any person who impersonates a Guardian, or procures a Kuya-Ate Guardian designation by fraud, shall suffer the penalty of *prision correccional in its maximum period and a fine of ₱300,000 to ₱1,000,000*.
- (d) The responsible officers of a covered platform who knowingly and willfully defies a final order under Section 22 shall suffer *imprisonment of six (6) months to two (2) years and a fine of ₱1,000,000 to ₱5,000,000*.
- (e) A child who commits an act under this Section shall be dealt with exclusively under Republic Act No. 9344, as amended. A child who merely acquires or uses a trafficked account shall incur no criminal liability and shall be referred for intervention.
- (f) Prosecution under this Section is without prejudice to liability under Republic Act No. 11930, Republic Act No. 10175, the Revised Penal Code, and other laws.

SEC. 25. Civil Liability to the Child. – A child who suffers harm from a contact that a covered platform's violation of Article II made possible may recover actual, moral, and exemplary damages from the platform. Proof of a material violation shall constitute *prima facie*

evidence of negligence, but the claimant shall still prove injury and causal connection. Nothing in this Section creates strict liability for an unavoidable act of a third person or for a platform's good-faith compliance with a lawful order.

The action may be brought by the child through a duly authorized representative, by the Guardian, or, on the child's behalf by the Public Attorney's Office or the Department of Social Welfare and Development. The action shall be filed within the period provided by the Civil Code or other applicable law. The period shall be suspended only to the extent expressly allowed by law.

SEC. 26. Privacy and Data Protection. – (a) Personal data processed under this Act, including data used for age assurance and for the verification of Guardians and Kuya-Ate Guardians, shall be limited to what is necessary; shall be kept separate from, and never used for, advertising, profiling, behavioral recommendation, or product development; and shall be securely deleted or de-identified when no longer necessary, under the supervision of the National Privacy Commission.

No covered platform shall retain an identity document or biometric information where a less intrusive method can reasonably achieve the same protection. Every covered platform shall provide a simple channel for correcting an erroneous age classification.

Automated processing of communications to or from child accounts may be undertaken only to the extent reasonably necessary to detect, prevent, block, or report conduct prohibited by this Act, after clear notice to users and subject to data minimization, human review of adverse action, access controls, auditability, and deletion when no longer necessary. Nothing in this Section authorizes interception or disclosure prohibited by Republic Act No. 4200, the Constitution, Republic Act No. 10173, Republic Act No. 10175, or the Rules of Court.

ARTICLE VI

GOVERNMENT, SCHOOL, AND COMMUNITY

SEC. 27. Implementing Office; Oversight. – The Department of Information and Communications Technology shall administer this Act through the office charged by law with the online safety of children; until such office is constituted, through the Cybercrime Investigation and Coordinating Center. It shall act in coordination with the National Telecommunications Commission, the National Privacy Commission, the Bangko Sentral ng Pilipinas, the Philippine National Police Anti-Cybercrime Group, the National Bureau of Investigation, the Department of Education, the Department of Social Welfare and Development, the Council for the Welfare of Children, and the National Youth Commission.

The Office shall report annually to Congress. On the fifth (5th) year of effectivity, the Office shall submit an independent evidence review of Section 6, and Congress shall determine whether the rule on voice features should be retained, tightened, or relaxed.

SEC. 28. Bantay-Laro sa Paaralan at Barangay. – The appropriate government departments and agencies shall, as provided below, take an active role in the implementation of this Act, by undertaking the following measures:

- (a) The Department of Education shall include a Guardian Console orientation in enrollment and in parent-teacher assemblies.
- (b) Every Barangay Council for the Protection of Children shall keep a Bantay-Laro help desk to assist Guardians in linking accounts and designating Kuya-Ate Guardians.
- (c) The National Youth Commission and the Sangguniang Kabataan shall organize Kuya-Ate Volunteers — young adults trained to assist households in their own barangays. Service may be credited under the National Service Training Program, as the implementing rules may provide.
- (d) Implementation shall begin with geographically isolated and disadvantaged areas, low-connectivity communities, and the poorest and most remote schools. Materials shall be available in print and in low-data formats.
- (e) No local government unit, public school, or public school personnel shall be required to procure technology, collect child-account data, or perform any function under this Section unless the corresponding funds, equipment, and training have been provided.

SEC. 29. Appropriations. – The amount of *Two Hundred Million Pesos (P200,000,000)* is hereby appropriated for the initial implementation of this Act, of which not less than *forty percent (40%)* shall fund Section 28. Thereafter, the amounts necessary shall be included in the annual General Appropriations Act.

ARTICLE VII FINAL PROVISIONS

SEC. 30. Transitory Provisions. – (a) Sections 5 to 8 shall be complied with within ninety (90) days from effectivity; all other duties of covered platforms, within one hundred eighty (180) days.

- (b) An existing child account without a Guardian link shall not be suspended. Its communication and discovery features shall remain closed until the link is made.
- (c) A covered platform under Section 4(b) shall have an additional *one hundred eighty (180) days* to comply with Articles III and V.

SEC. 31. Implementing Rules and Regulations. – Within ninety (90) days from effectivity, the Department of Information and Communications Technology, in consultation with the agencies in Section 27, children and youth, parents' organizations, educators, persons with disabilities, child-rights and privacy organizations, and industry including micro, small, and medium enterprises, shall issue the implementing rules. The rules shall not authorize the

collection or use of personal data beyond what this Act permits. Sections 5, 6, 7, 8, 9, 10, 15, 16(b), 18, 19, 24, and 25 are self-executing and shall take effect even without such rules.

SEC. 32. Relationship to Other Laws. – This Act supplements Republic Act No. 7610, Republic Act No. 9775, Republic Act No. 11930, Republic Act No. 10175, Republic Act No. 10173, Republic Act No. 9344, and the Family Code. Where this Act and another law cover the same conduct, the provision more protective of the child shall prevail.

Any law regulating the access of children to social media and online gaming platforms, and any law strengthening Republic Act No. 11930, whether enacted before or after this Act, shall be read together with it. Any office, registry, age-assurance framework, or resident-representative system created by such law shall serve the purposes of this Act, and no covered platform shall be required to comply twice with the same requirement.

SEC. 33. Separability Clause. – If any provision of this Act is declared unconstitutional or invalid, the other provisions not affected shall remain in full force and effect.

SEC. 34. Repealing Clause. – All laws, decrees, orders, rules, and regulations inconsistent with this Act are hereby repealed or modified accordingly.

SEC. 35. Effectivity. – This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,