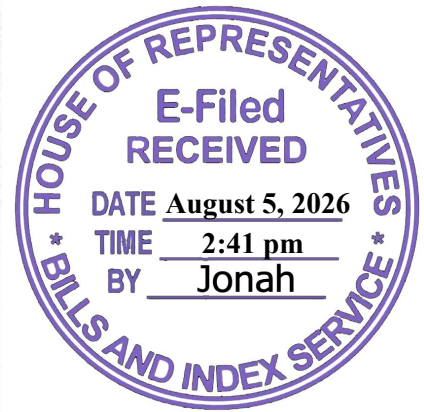


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Philippines

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 10635



INTRODUCED BY REP. MARCELINO "MARCY" R. TEODORO

EXPLANATORY NOTE

Republic Act No. 10175, otherwise known as the Cybercrime Prevention Act of 2012, was enacted to address crimes committed through information and communications technologies. Since its passage, however, the digital landscape has evolved dramatically. Social media platforms have become the principal venues for public discourse, political engagement, business, education, and personal interaction. Alongside these developments has emerged an alarming rise in coordinated online harassment, malicious digital intimidation, cyber mobbing, doxxing, and sustained campaigns of abuse designed to silence, humiliate, threaten, or psychologically harm individuals.

While existing laws penalize offenses such as libel, identity theft, illegal access, and computer-related fraud, they do not comprehensively address organized patterns of online abuse that exploit social media platforms to inflict substantial emotional, reputational, and even physical harm. Victims often include journalists, educators, medical professionals, lawyers, judges, public servants, women, children, members of vulnerable sectors, and ordinary citizens who become targets of coordinated digital attacks.

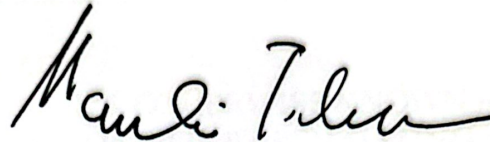
This proposed measure seeks to strengthen the Cybercrime Prevention Act by criminalizing clearly defined forms of coordinated online abuse while maintaining full respect for the constitutional guarantees of freedom of speech, freedom of the press, and the free exchange of ideas.

The widespread accessibility of social media, online gaming platforms, livestreaming services, and other digital technologies has likewise enabled the proliferation of dangerous online challenges, violent digital content, coordinated hate campaigns, malicious disinformation directed against private individuals, and online activities that encourage self-harm, suicide, unlawful violence, and other criminal conduct. These emerging threats, particularly to children and vulnerable sectors, demand a calibrated legal response that protects public safety while fully respecting constitutionally protected freedoms.

Nothing in this Act shall be construed as restricting legitimate criticism, political dissent, satire, public advocacy, journalistic reporting, whistleblowing, academic discussion, or expressions made in good faith on matters of public concern. The measure penalizes only conduct that intentionally weaponizes digital platforms to threaten, terrorize, harass, expose sensitive personal information without lawful authority, or incite unlawful acts against another person.

By updating our cybercrime laws to meet modern digital realities while safeguarding constitutional liberties, this measure promotes a healthier, safer, and more responsible online environment for all Filipinos.

Approval of this bill is earnestly sought.



HON. MARCELINO "MARCY" R. TEODORO

Representative

1st District, Marikina City

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Philippines

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 10635

INTRODUCED BY REP. MARCELINO "MARCY" R. TEODORO

AN ACT
STRENGTHENING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE
"CYBERCRIME PREVENTION ACT OF 2012," BY PENALIZING
COORDINATED ONLINE HARASSMENT, DIGITAL INTIMIDATION,
MALICIOUS DOXXING, AND OTHER FORMS OF ABUSIVE ONLINE
CONDUCT, PROVIDING SAFEGUARDS FOR FREEDOM OF EXPRESSION,
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 "Online Safety and Digital Responsibility Act"

SECTION 2. Declaration of Policy.

It is hereby declared the policy of the State to:

- (a) protect every person's dignity, privacy, safety, mental health, and digital well-being;
- (b) safeguard children and other vulnerable persons from harmful online activities;
- (c) promote responsible digital citizenship;
- (d) preserve freedom of speech, freedom of the press, academic freedom, artistic expression, and legitimate political discourse; and
- (e) ensure that digital technologies are not used to terrorize, threaten, intimidate, unlawfully expose private information, encourage violence, or promote self-harm.

SECTION 3. Amendment.

Republic Act No. 10175 is hereby amended by inserting new prohibited cyber offenses, to read as follows:

A. Coordinated Online Harassment

Any person or group who, through a computer system, social media platform, messaging application, or similar digital technology, intentionally organizes, directs, finances, or knowingly participates in a coordinated campaign of repeated harassment, intimidation, or threats against another person for the purpose of causing substantial emotional distress, fear for personal safety, or unlawful interference with the lawful exercise of rights shall be liable under this Act.

For purposes of this section, a "coordinated campaign" refers to a planned or organized effort involving multiple persons, accounts, pages, bots, or automated systems acting in concert.

B. Digital Hate Campaigns

Any person who intentionally organizes, finances, directs, or knowingly participates in a coordinated digital campaign that incites imminent unlawful violence, persecution, or criminal acts against any person or identifiable group through repeated threats, intimidation, or unlawful harassment shall be liable under this Act.

C. Malicious Digital Doxxing

Any person who intentionally publishes or disseminates another person's home address, personal telephone number, financial information, government-issued identification numbers, location data, family information, or other sensitive personal information without lawful authority and with intent to threaten, intimidate, facilitate harassment, or expose such person to danger shall be punished under this Act.

Disclosure made pursuant to law, court order, official government functions, or legitimate journalism in the public interest shall not constitute an offense.

D. Digital Incitement to Unlawful Violence

Any person who intentionally uses digital platforms to encourage or direct imminent unlawful violence or criminal acts against a specific person or identifiable group shall be liable under this Act.

E. Promotion of Dangerous Digital Challenges

Any person who knowingly creates, administers, distributes, finances, or intentionally promotes any online challenge, digital activity, or interactive content designed to encourage or induce: suicide; self-harm; violence against another person; acts of terrorism; child exploitation; other criminal acts, where such conduct poses a substantial risk of physical injury or death, shall be liable under this Act.

F. Harmful Violent Digital Games

Any person who knowingly develops, distributes, operates, or intentionally makes available in the Philippines any digital game or online application whose primary purpose is to encourage or reward suicide, self-harm, unlawful violence, terrorism, or criminal conduct shall be liable under this Act.

This provision shall not apply to educational, military, law enforcement, scientific, historical, artistic, or cinematic simulations that do not intentionally promote unlawful conduct.

G. Use of Automated Accounts for Digital Harassment.

The knowing use of automated accounts, fake accounts, bot networks, or similar technological means to amplify coordinated harassment or intimidation shall constitute an aggravating circumstance.

SECTION 4. Aggravating Circumstances

The following shall increase the penalty:

- use of bot networks;
- use of artificial intelligence to generate abusive content;
- anonymous mass reporting intended to silence another person;
- victim is a child;
- victim is a senior citizen;
- victim is a person with disability;
- victim is targeted because of official duties;
- offense committed by an organized group.

SECTION 5. Duties of Digital Platforms

Digital platforms, online gaming providers, social networking services, messaging services, and similar online intermediaries operating in the Philippines shall: establish accessible complaint mechanisms; preserve electronic evidence upon lawful request; comply with lawful court orders; remove unlawful content upon final lawful determination; publish annual transparency reports; implement reasonable safeguards against bot networks and coordinated digital abuse; implement age-appropriate safety measures protecting minors from content promoting suicide, self-harm, unlawful violence, or criminal conduct. Compliance with this section shall always be subject to the Constitution, the Data Privacy Act, due process, and lawful judicial process.

SECTION 6. Administrative Liability of Platforms

Failure to comply with lawful orders under this Act may subject digital platforms to

SECTION 7. Assistance to Victims.

The Department of Information and Communications Technology, the Philippine National Police Anti-Cybercrime Group, the National Bureau of Investigation Cybercrime Division, and the Department of Justice shall establish expedited mechanisms for receiving complaints, preserving electronic evidence, and extending assistance to victims.

SECTION 8. Digital Citizenship Education

The DepEd, CHED, TESDA, DICT, DOJ, and DSWD shall jointly develop nationwide educational programs promoting responsible online behavior, digital literacy, cyber safety, mental health awareness, and the prevention of cyberbullying, online hate campaigns, digital manipulation, dangerous online challenges, and violent digital content.

SECTION 9. Freedom of Expression Safeguards

Nothing in this Act shall be construed to prohibit or penalize:

- (a) legitimate criticism of public officials;
- (b) political advocacy;
- (c) peaceful protests;
- (d) journalistic reporting;
- (e) whistleblowing;
- (f) satire;
- (g) parody;
- (h) academic discussion;
- (i) religious expression;
- (j) artistic expression;
- (k) good-faith commentary on matters of public concern.

No person shall incur criminal liability solely for expressing an opinion absent proof beyond reasonable doubt that the expression intentionally constituted conduct expressly prohibited under this Act.

SECTION 10. Penalties

Any person found guilty shall suffer imprisonment and fines corresponding to the gravity of the offense, without prejudice to liability under the Revised Penal Code, the Data Privacy Act, the Safe Spaces Act, the Anti-Photo and Video Voyeurism Act, and other applicable laws.

Where the victim is a child, senior citizen, person with disability, judge, prosecutor, lawyer, journalist, healthcare worker, teacher, law enforcement officer, election officer, or public official targeted by reason of the lawful discharge of official duties, the penalty shall be imposed in its maximum period.

SECTION 11. Implementing Rules and Regulations.

Within ninety (90) days from the effectivity of this Act, the Department of Justice and the Department of Information and Communications Technology shall promulgate the implementing rules and regulations.

SECTION 12. Separability Clause.

If any provision of this Act is declared unconstitutional, the remaining provisions shall remain in full force and effect.

SECTION 13. Repealing Clause.

All laws, decrees, executive orders, rules, and regulations inconsistent with this Act are hereby repealed or modified accordingly.

SECTION 14. Effectivity.

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