



REPUBLIC OF THE PHILIPPINES
House of Representatives
CONSTITUTION HILLS, QUEZON CITY

TWENTIETH CONGRESS
First Regular Session

House Bill No. **8734**



AN ACT PROVIDING FOR THE FAIR AND ACCOUNTABLE USE OF SOCIAL MEDIA, ARTIFICIAL INTELLIGENCE AND INTERNET TECHNOLOGY FOR THE HOLDING OF FREE, ORDERLY, HONEST, PEACEFUL AND CREDIBLE ELECTIONS, PROVIDING PENALTIES FOR VIOLATIONS THEREOF, AND FOR OTHER PURPOSES

Introduced by Representative SHIRLYN L. BAÑAS-NOGRALES

EXPLANATORY NOTE

The rapid expansion of social media, artificial intelligence (AI), and digital technologies has fundamentally transformed the Philippine electoral landscape. While these platforms offer unprecedented opportunities for voter engagement and democratic participation, they also present serious risks. The current Fair Elections Act (R.A. 9006), enacted in 2001, predates the era of AI-generated “deepfakes,” coordinated inauthentic behavior, bot networks, and the instantaneous spread of viral disinformation.

This legislative gap has been exploited, enabling disinformation campaigns that erode public trust, manipulate voter behavior, and threaten the integrity of elections.

This Bill seeks to establish a comprehensive, modern, and forward-looking legal framework that addresses the realities of digital-era elections. It introduces clear mechanisms for accountability, transparency, and the protection of both candidates and the electorate, including mandatory disclosure of AI-generated campaign materials and the monitoring of online election expenditures.

Key features of this Bill include:

1. Permanent Enforcement Body – Creation of the Digital Election Crimes Unit (DECU) within the COMELEC, staffed with legal and technical experts to monitor and act continuously during election periods.
2. Rapid Takedown Authority – Empowerment of COMELEC to issue mandatory 24-hour takedown orders for high-harm content, such as AI-generated deepfakes, false election schedules, or incitements to violence.
3. Platform Accountability – Imposition of significant administrative fines on social media platforms and internet providers that fail to comply with valid takedown orders, including the requirement of a local, on-call legal representative to receive such orders.
4. Transparency in Campaign Financing – Establishment of a publicly accessible Political Ad Library, mandatory real-world verification of advertisement sponsors, and prohibition of foreign funding for online election propaganda.

5. Public Digital Literacy and Resilience – Creation of a Digital Literacy and Anti-Disinformation Trust Fund, financed by penalties collected under this Act, to support media literacy curricula and nationwide public awareness campaigns on identifying disinformation and malicious digital content.

This Act provides the COMELEC with the necessary tools to regulate online campaign activities, prosecute the use of malicious digital technologies, and safeguard the electorate against deception and manipulation.

For these reasons, the immediate passage of this Bill is earnestly sought.


SHIRLYN L. BAÑAS-NOGRALES



REPUBLIC OF THE PHILIPPINES
House of Representatives
CONSTITUTION HILLS, QUEZON CITY

TWENTIETH CONGRESS
First Regular Session

House Bill No. **8734**

Introduced by Representative SHIRLYN L. BAÑAS-NOGRALES

AN ACT PROVIDING FOR THE FAIR AND ACCOUNTABLE USE OF SOCIAL MEDIA, ARTIFICIAL INTELLIGENCE AND INTERNET TECHNOLOGY FOR THE HOLDING OF FREE, ORDERLY, HONEST, PEACEFUL, AND CREDIBLE ELECTIONS, PROVIDING PENALTIES FOR VIOLATIONS THEREOF, 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 “*Artificial Intelligence and Digital Platforms in Elections Act of 2026.*”

SECTION 2. *Declaration of Policy.* – It is the policy of the State to ensure free, honest, fair, peaceful, and credible elections by regulating the use of digital technologies, including social media and artificial intelligence, to protect the democratic process and the informed exercise of the right to vote and strengthen digital literacy and public resilience.

SECTION 3. *Definition of Terms.* – As used in this Act:

- a.) *Artificial Intelligence (AI) Technology* refers to computer systems or machines that simulate human intelligence processes with a focus on learning, reasoning, problem-solving, perception, use of language, and image manipulation;
- b.) *Astroturfing* refers to a practice designed to mask the source of a message so that it appears as though it has broad support from grassroots participants, rather than originating from a small group or organization;
- c.) *Bot* refers to a software program or computer system designed to perform automated, repetitive, pre-defined tasks on the internet, often used on social media to simulate or imitate human user behavior;
- d.) *Candidate* refers to any person seeking an elective public office who has filed a certificate of candidacy, as defined in the Omnibus Election Code ;
- e.) *Cheapfakes* refer to forms of visual disinformation for which authentic images or videos are re-contextualized to deliberately alter their meaning;
- f.) *Coordinated Inauthentic Behavior* refers to deliberate and coordinated actions carried out by individuals, groups, or organizations to deceive or mislead the public by spreading false, misleading, or manipulated information online;
- g.) *Deepfakes* refer to digitally manipulated images, videos, or audio files created using artificial intelligence to fabricate realistic representations of people, events, or statements and falsely make it appear that an action, statement, or event transpired but did not occur in reality;
- h.) *Digital Election Crimes Unit (DECU)* refers to the permanent office within the Commission on Elections (COMELEC) created under this Act, responsible for

- monitoring, investigating, and enforcing digital election laws;
- i.) *Digital Platform* refers to any social media platform, website, mobile application, or internet-based service that allows users to create, share, or interact with content;
 - j.) *Disinformation* refers to false information that is spread, or information that is based on fact but removed from its original context, and is maliciously manipulated and used in a partisan political activity with the intent to mislead, harm, or manipulate public opinion or voter behavior;
 - k.) *Election Campaign or Partisan Political Activity* refers to any act designed to promote the election or defeat of a particular candidate, as defined in the Omnibus Election Code;
 - l.) *Electoral Ads and Electoral Posts* refer to advertisements and social media posts that have for their primary purpose the promotion of the victory or defeat of a candidate;
 - m.) *Fake Social Media Accounts* are social media profiles created using false, misleading, or inauthentic identities, often with the intent to mislead, manipulate, or influence public opinion or voter behavior;
 - n.) *Foreign Interference* refers to any act by a foreign individual, entity, or government to directly or indirectly fund, sponsor, create, or disseminate election propaganda for or against any candidate;
 - o.) *Malicious and Deceptive Content* refers to a specific category of prohibited content defined as: (1) AI-generated deepfakes of a candidate; (2) digital content that incites imminent violence, terrorism, or public disorder; or (3) digital content that disseminates materially false and alarming information regarding election schedules, polling places, or the conduct of the election;
 - p.) *Micro-targeting* refers to a form of targeting online advertisements that uses technological developments to analyze a person's online usage to preferentially serve advertisements and other information that specifically reflect that individual user's preferences and personality;
 - q.) *Misinformation* refers to false or inaccurate information that is spread in a partisan political activity, regardless of whether there is intent to mislead;
 - r.) *Political Ad Library* refers to a publicly accessible, searchable, and real-time database maintained by a digital platform, which contains all electoral ads, their content, sponsor, cost, and targeting data; and
 - s.) *Social Media Associates* refer to contractors, including paid digital influencers and online content creators, whose primary duty is to promote the election or defeat of any candidate through social media interactions and engagement.

SECTION 4. *Use of the Internet and Social Media as Lawful Election Propaganda.* – Political advertisements and election propaganda disseminated through the internet and social media are hereby recognized as legitimate platforms for candidates and political parties to engage with the electorate. Such use shall be subject to limitations on authorized campaign expenses, adherence to truth in advertising, and compliance with all other rules and regulations issued by the Commission on Elections (COMELEC) to ensure fair and orderly elections.

SECTION 5. *Requirements and Limitations on the Use of Election Propaganda.* – The use of the internet and social media for election propaganda shall be subject to the following conditions:

- a.) Each registered political party and candidates shall register with the COMELEC the website name and web address of all platform-verified official accounts, websites, and social media pages within thirty (30) days from the last day for the

filing of Certificates of Candidacy.

- b.) Any other website or social media page not registered but which, when taken as a whole, has for its primary purpose the endorsement of a candidate, shall be considered an additional official page of the said candidate for regulatory and campaign expenditure purposes.
- c.) Only verified accounts, websites, blogs, and/or social media pages may run electoral ads and boost or promote electoral posts.
- d.) Micro-targeting of electoral ads shall not be allowed. Electoral ads may only be targeted using the criteria of geographical location (except radius targeting), age, and gender.

SECTION 6. *Transparency and Disclosure Requirements on the Use of Artificial Intelligence (AI) Technology.* – The use of Artificial Intelligence (AI) technology in election propaganda shall comply with the following requirements:

- a.) All election propaganda and campaign materials of candidates and political parties that utilize AI technology shall clearly and conspicuously disclose such use through a visible or audible, and reasonably permanent, watermark or disclaimer; and
- b.) The required disclosure shall explicitly state that the content has been generated, created, or materially manipulated using AI, and shall remain visible or audible for the entire duration of publication of the material.

SECTION 7. *E-Rallies and Livestreams.* – Political parties and candidates may conduct peaceful online political meetings, rallies, and other analogous activities during the election period. Live streaming conducted through a candidate's duly registered social media platform shall be considered an e-rally for purposes of this Act.

Candidates may receive voluntary in-platform gifts or contributions from viewers; however, they shall be prohibited from giving gifts, monetary incentives, or any form of consideration to livestream audiences, or from conducting promotions, contests, or similar activities that grant rewards, currency, or items of value to platform users.

SECTION 8. *Legitimate Expressions by Private Individuals.* – The expression of personal opinions for or against a candidate, commentary on matters of public concern, discussion of electoral issues, when undertaken independently and without coordination with any candidate, political party, or partisan group, shall not be deemed election propaganda or partisan political activity within the contemplation of this Act. Nothing herein shall be construed to abridge, restrict, or diminish the constitutionally guaranteed freedom of speech, expression, or of the press.

SECTION 9. *Prohibited Acts.* – The following acts shall be unlawful and shall constitute an election offense:

- a.) The use of false amplifiers, including fake accounts, bots, and Astroturf groups, to spread disinformation or misinformation for or against any candidate or political party;
- b.) Engaging in coordinated inauthentic behavior intended to manipulate public opinion or voter behavior;
- c.) The creation, dissemination, or promotion of deepfakes, cheapfakes, or soft fakes to undermine the electoral process or to campaign for or against any candidate;
- d.) The use of content generated or materially manipulated through artificial intelligence in violation of the mandatory transparency and disclosure requirements under Section 6 of this Act;

- e.) The creation, dissemination, or promotion of fake news or disinformation designed to mislead, harm, or manipulate public opinion or voter behavior;
- f.) The use of fake, unregistered, or unauthorized social media accounts to conduct partisan political activity;
- g.) Engaging in foreign interference, including any act where a foreign individual, government, or entity directly or indirectly funds, sponsors, purchases, or creates election propaganda for or against any candidate or political party; and
- h.) Creating, propagating, or disseminating malicious and deceptive digital content as defined in Section 3(o) of this Act.

SECTION 10. *Creation of Digital Election Crimes Unit (DECU).* – There is hereby created a permanent Digital Election Crimes Unit (DECU) under the direct supervision of the COMELEC En Banc. The DECU shall be composed of legal experts, data scientists, and digital forensic investigators, and shall serve as the lead office responsible for operating the National Public Reporting Portal, coordinating with digital platforms, and providing technical and evidentiary support for the investigation and prosecution of offenses under this Act.

SECTION 11. *National Public Reporting Portal.* – The DECU shall establish and maintain a 24/7 National Public Reporting Portal where any citizen can anonymously report suspected violations of this Act, including malicious content, bot networks, and undisclosed paid promotion.

SECTION 12. *Takedown Procedures.* – Upon receipt of a verified report or complaint, the DECU shall act in accordance with the following procedures:

- a.) **Standard Procedure.** – In cases involving alleged violations of Section 5 (Registration) or Section 6 (AI Disclosure), the DECU shall:
 - i. Conduct an initial assessment to determine the sufficiency and verifiability of the report within a reasonable period;
 - ii. Where a *prima facie* case exists, issue a show-cause order to the alleged violator, directing the submission of a verified explanation within a non-extendible period to be prescribed by the COMELEC;
 - iii. Evaluate the evidence and explanation submitted, and, when necessary, require the submission of additional information or conduct summary proceedings; and
 - iv. Upon a finding of violation, issue a written determination and formally request the concerned digital platform, intermediary, or Internet Service Provider (ISP) to remove, restrict access to, or disable the subject content, account, or material within a specified period.
- b.) **Urgent Twenty-Four (24)-Hour Takedown Procedure.** – In cases involving content that is *prima facie* determined by the DECU to constitute malicious and deceptive content under Section 9(h) of this Act, the COMELEC shall:
 - i. Undertake expedited verification and documentation of the reported content;
 - ii. Issue an immediate and mandatory takedown order, supported by a brief statement of factual and legal basis, directed to the relevant digital platform, intermediary, or ISP; and
 - iii. Require the concerned entity to remove, disable access to, or otherwise restrict the subject content within twenty-four (24) hours from receipt of the order.

Compliance with takedown orders issued under this Section shall be without prejudice to the conduct of further administrative or criminal proceedings, and subject to such remedies as may be available under existing laws, rules, and regulations.

SECTION 13. *Platform and ISP Liability.* – Any social media platform, internet company, or ISP that fails to comply with a valid takedown order issued by COMELEC under Section 12(b) shall be administratively liable. A fine of not less than One Million Pesos (₱1,000,000.00) shall be imposed for every twelve (12)-hour period of continued non-compliance following the lapse of the twenty-four (24)-hour compliance deadline, without prejudice to the imposition of any appropriate civil or criminal liabilities under this Act and existing law.

SECTION 14. *Mandated Local Point of Contact.* – Any social media company, internet company, or digital platform with more than one million (1,000,000) registered users in the Philippines shall establish a Philippine-based public policy and enforcement team, or alternatively, designate a duly authorized legal representative within the country, vested with full authority to receive, acknowledge, and promptly act on all administrative and legal orders issued by the COMELEC pursuant to this Act.

SECTION 15. *Public Political Ad Library.* – All digital platforms that accept payment for electoral ads shall be required to maintain a real-time, publicly accessible, and searchable Political Ad Library. This library shall contain, at a minimum:

- a.) A digital copy of the electoral ad;
- b.) The name of the person or entity who paid for the ad;
- c.) The total amount spent on the ad; and
- d.) The basic targeting criteria used (age, gender, and geographical location).

SECTION 16. *Mandatory Verification of Ad Sponsor.* – No digital platform shall accept payment for any electoral advertisement unless it has first obtained and verified the following information from the ad sponsor:

- a.) For an individual, the full name, residential address, Taxpayer Identification Number (TIN), and business registration or permit, if applicable; and
- b.) For an entity, the full registered name, business registration or permit, business address, TIN of the entity, and the names of its corporate officers.

All verified information shall be maintained by the platform and shall be made readily available to the COMELEC upon request.

SECTION 17. *Reporting Requirements of Contractors and Social Media Associates.* – To ensure transparency and the accurate determination of actual election expenditures in accordance with the R.A. No. 9006 (Fair Elections Act), all social media associates, such as contractors, paid digital influencers, online content creators, and business firms shall submit to the COMELEC certified true copies of all contracts, invoices, receipts, and reports relating to electoral spending in accordance with COMELEC rules and regulations. Internet and social media platforms shall likewise provide the COMELEC with complete and verifiable information on all paid advertisements placed by candidates or political parties, including the identity of the sponsor, the content of the advertisement, political ad time and space, and the amount expended, to enable effective monitoring and enforcement of campaign finance rules.

SECTION 18. *Digital Literacy and Anti-Disinformation Trust Fund and its Administration.* – There is hereby created Digital Literacy and Anti-Disinformation Trust Fund, into which all administrative fines and penalties collected from violations of any provision of this Act shall be automatically remitted.

The Fund shall be under the joint administration of the Department of Information and Communications Technology (DICT), the Department of Education (DepEd), the

Commission on Higher Education (CHED), and the Department of the Interior and Local Government (DILG). The Fund shall be used exclusively for programs and projects that advance digital literacy and public resilience against disinformation, including:

- a.) The development, integration, and implementation of a mandatory media literacy and digital citizenship curriculum in all basic and higher education institutions; and
- b.) The creation and conduct of nationwide public awareness campaigns to educate citizens on identifying disinformation, AI-generated content, and other forms of malicious online behavior.

SECTION 19. *Penalty.* – Any person who violates Section 5, 6, 7, 9, 15, 16, or 17 of this Act shall be guilty of an election offense and, upon conviction, shall be punished by imprisonment of not less than one (1) year but not more than six (6) years without eligibility for probation, and shall likewise be required to pay a fine of not less than One Hundred Thousand Pesos (₱100,000.00). This penalty is in addition to the administrative fines prescribed under Section 13 of this Act.

Candidates for public office who are found guilty violating this Act shall, in addition to the penalties prescribed above, be perpetually disqualified from holding any public office and shall be deprived of the right to vote.

Public officers or employees who are found guilty under this Act shall, in addition to the penalties prescribed above, be perpetually disqualified from holding any public office and shall be deprived of the right to vote.

SECTION 20. *Appropriations.* – The amount necessary for the initial implementation of this Act, including the establishment of the Digital Election Crimes Unit (DECU) and the development of the National Public Reporting Portal, shall be charged against the current year's appropriations of the COMELEC. Thereafter, such sums as may be necessary for the continued implementation of this Act shall be included in the annual General Appropriations Act.

SECTION 21. *Right of Reply.* – All candidates and parties shall have the right to reply to charges published or disseminated against them. The digital platform, website, or social media account where the original malicious or deceptive content was published shall, upon order of the COMELEC, accord the aggrieved party the right of reply with the same prominence and placement as the offending content, free of charge, and without delay.

SECTION 22. *Implementing Rules and Regulations (IRR).* – Within ninety (90) days from the effectivity of this Act, the COMELEC, in consultation with the Department of Information and Communications Technology (DICT), National Telecommunications Commission (NTC), National Privacy Commission (NPC), Philippine National Police – Anti Cybercrime Group (PNP-ACG), the National Bureau of Investigation (NBI), the Department of Education (DepEd), the Commission on Higher Education (CHED), and the Department of the Interior and Local Government (DILG), and other relevant stakeholders, shall promulgate the necessary rules and regulations for the effective implementation of this Act.

SECTION 23. *Separability Clause.* – If any provision of this Act is declared invalid or unconstitutional, such declaration shall not affect the validity of the other provisions hereof.

SECTION 24. *Repealing Clause.* – All laws, decrees, rules, and regulations inconsistent with the provisions of this Act are hereby repealed, modified, or amended accordingly.

SECTION 25. *Effectivity.* – This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,