



HOUSE OF REPRESENTATIVES

H. No. 9465

BY REPRESENTATIVES MARCOS, DY (F.), ROMAN, SUAN, VILLAFUERTE (M.L.), SAKALURAN, YAMSUAN, HERNANDEZ (C.A.), CO-PILAR, RAMA, VARGAS, ARENAS, PUMAREN, JAVIER, GUINTU, MERCADO-REVILLA, REVILLA (B.), REVILLA (R.J.), RIVERA, LOYOLA, PLEYTO, ARROGANCIA, SOLON, VILLARICA, MONTES, PADIERNOS, RODRIGUEZ (R.), RODRIGUEZ (M.), HERNANDEZ (R.), GARCIA (A.), VILLANUEVA, TARRIELA, SALCEDA, CELESTE, BARONDA, BARBERS, PASCUAL, BANCORO, ATAYDE, MANGUDADATU, BARBA, OLIVAREZ, ACOSTA, VERGARA, GONZALES (A.), AUMENTADO, LAGBAS, ORETA, LACSON, DOMINGO, ORDANES, DEGAMO, GATCHALIAN, BERNOS (J.), LEDESMA, GOMEZ, YAP (ERIC), YAP (EDVIC), ODUCCADO, TAN (K.M.), VILLAFUERTE (V.R.L.), HORIBATA, RIDON, PUNO, VELOSO-TUAZON, MASTURA, MARQUEZ, EMANO, ORTEGA, MATIBAG AND TOLENTINO

AN ACT

PROHIBITING THE DELIBERATE DISSEMINATION OF FALSE INFORMATION THAT POSES VERIFIABLE PUBLIC HARM OR SERIOUS THREAT TO NATIONAL SECURITY, ESTABLISHING DIGITAL PLATFORM ACCOUNTABILITY AND TRANSPARENCY MECHANISMS, AND PROMOTING MEDIA AND DIGITAL LITERACY

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

CHAPTER I GENERAL PROVISIONS

SECTION 1. Short Title. – This Act shall be known as the “Digital Media Anti-False Information Act”.

SEC. 2. Declaration of Policy. – The State upholds the freedom of speech, of expression, and of the press, as guaranteed under Article III, Section 4 of the Constitution. It also recognizes the need to protect the public and the State from serious, malicious, and demonstrable effects of the intentional dissemination of false information through digital media that poses verifiable public harm and serious threat to national security. This Act seeks to deter and penalize such conduct as well as establish transparency, accountability, due process, and risk-mitigation standards for digital platforms.

CHAPTER II
DEFINITION OF TERMS

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

- (a) *Ad repository* refers to a searchable, publicly accessible database maintained by platforms that includes information on all paid advertisements, including the content, sponsor identity, payor, targeting criteria, expenditure, and dates of display;
- (b) *Adequate disclosure* refers to a clear and conspicuous notice that:
 - (1) Identifies the content as synthetically generated, materially altered, or manipulated;
 - (2) Is displayed in the content itself, in accompanying metadata, labeling, watermarking, captioning, or other reasonable effective means;
 - (3) Is readily visible or accessible to an ordinary user prior to or during viewing of the content; and
 - (4) Is not hidden, obscured, misleading or designed to be easily removed or overlooked;
- (c) *Certified out-of-court dispute settlement (ODS) body* refers to an independent institution accredited by the Department of Information and Communications Technology (DICT) to provide accessible, impartial, and non-binding dispute resolution services for user appeals of platform decisions;
- (d) *Content* refers to any text, image, audio recording, video, animation, or other digital material published on digital platforms;
- (e) *Coordinated inauthentic behavior (CIB)* refers to the organized use of fake accounts, impersonation, bots, deceptive networks, or concealed sponsorship to manipulate public discourse, spread falsehoods, or interfere with democratic processes, which includes to troll, click, engagement and account farms;
- (f) *Dark patterns* refer to deceptive, manipulative, or coercive interface designs that materially distort or impair a user's ability to make free, informed, and autonomous choices, such as misleading consent flows, hidden settings, or default opt-ins;
- (g) *Digital media* refers to any form of communication or content that is created, stored, and distributed using electronic devices and computer networks;

- 1 (h) *Digital platform* refers to any online service such as a social media network,
2 messaging service, search engine, and content-sharing platform that enables
3 users to create, upload, access, rank, recommend, share, or disseminate
4 content to users in the Philippines;
- 5 (i) *Disinformation* refers to false or misleading factual information deliberately
6 created, materially altered, or disseminated with knowledge of falsity or reckless
7 disregard for truth, and with intent to cause serious public harm;
- 8 (j) *Dissemination* refers to the act of spreading information or knowledge so that it
9 reaches many people;
- 10 (k) *Fact-checking organization* refers to an independent, non-partisan entity
11 accredited either by international fact-checking bodies such as the International
12 Fact-Checking Network, or recognized Philippine media organizations to
13 review, verify, and assess the accuracy of information published and
14 disseminated in online platforms;
- 15 (l) *Fake account* refers to an account that intentionally misrepresents the identity
16 of a real or fictitious person for the purpose of deceiving users regarding the
17 source, authenticity, affiliation, or sponsorship of content;
- 18 (m) *False information* refers to any information that is demonstrably false and presented
19 as fact;
- 20 (n) *Independent audit* refers to an assessment carried out by an external, qualified,
21 and independent auditor to evaluate a platform's compliance with its obligations
22 under this Act, including transparency, risk assessment, and mitigation
23 measures;
- 24 (o) *Lawful excuse* refers to circumstances in which noncompliance results from:
- 25 (1) Compliance with another applicable law, judicial order, or binding legal
26 obligation;
- 27 (2) *Force majeure* or extraordinary events beyond reasonable control;
- 28 (3) Technical impossibility, cybersecurity risks, or system integrity
29 concerns despite reasonable diligence;
- 30 (4) Materially defective, unauthorized, or legally insufficient government
31 requests; or
- 32 (5) Other comparable circumstances demonstrating good-faith inability
33 rather than willful refusal to comply;

- 1 (p) *Malicious intent* refers to the deliberate or reckless disregard for truth, with the
2 purpose of causing serious harm to the public or threat to national security;
- 3 (q) *Manipulated media* refers to digital content such as image, video, or audio that
4 has been deliberately edited, synthesized, or generated by artificial intelligence
5 (AI) to mislead viewers;
- 6 (r) *Materially assist* refers to knowingly providing substantial operational, financial,
7 technical, or logistical support;
- 8 (s) *Notice-and-action* mechanism refers to a standardized electronic system
9 operated by platforms that enables users to submit notices of allegedly illegal
10 content and requires platforms to act upon and communicate the result of such
11 notices;
- 12 (t) *Publication* refers to the act of uploading content on a digital platform with an
13 intent to circulate particular information to the public;
- 14 (u) *Reckless disregard* for truth refers to publication despite serious doubts as to
15 the truthfulness of the information, or deliberate avoidance of readily available
16 facts indicating probable falsity. It does not include mere negligence, mistake,
17 poor judgment, failure to investigate fully, reliance on a source later proven
18 incorrect, or good-faith interpretation of incomplete or conflicting information;
- 19 (v) *Recommender system* refers to an automated system used by platforms to
20 determine the ranking, ordering, or prioritization of information displayed to
21 users, based on profiling, engagement, or other algorithmic criteria;
- 22 (w) *Risk assessment* refers to a structured evaluation conducted annually by the
23 Very large online platform in the Philippines (VLP-PH) to identify, measure, and
24 document systemic risks related to disinformation, manipulation, civic
25 discourse, protection of minors, and election integrity;
- 26 (x) *Serious threat to national security* refers to any activity resulting in, or creating
27 a clear and present danger that:
- 28 (1) Compromise military operations, intelligence activities, or classified
29 defense information;
- 30 (2) Interfere with the conduct of free and fair elections, such as:
- 31 (i) Disseminating false announcements that election day has been
32 postponed;

- 1 (ii) Publishing fake Commission on Elections (COMELEC) advisories
2 changing polling locations or voting procedures;
- 3 (iii) Falsely announcing that a candidate has withdrawn or be disqualified;
- 4 (iv) Disseminating fabricated election results intended to suppress voter
5 turnout; or
- 6 (v) Creating fake COMELEC websites, social media accounts, or official
7 notices;
- 8 (3) Materially impair the lawful operations of government through unlawful
9 acts involving violence, sabotage, or fraud; or
- 10 (4) Incite or facilitate violence, sabotage, or armed hostility;
- 11 (y) *Social media platform* refers to any online service, website, or application that:
- 12 (1) Enables users to create, upload, share, or disseminate user-generated.
13 content, including but not limited to text, images, videos, and live
14 broadcasts; or
- 15 (2) Allows for the interaction of users through features such as likes,
16 comments, shares, or similar mechanisms;
- 17 (z) *Verifiable public harm* refers to material, concrete, and objectively
18 demonstrable injury to public health and public safety, and not based on mere
19 offense, confusion, speculation, political disagreements, or reputational injury.
20 Verifiable public harm may include the following:
- 21 (1) Imminent and demonstrable risk to life, health, or physical safety,
22 including interference with emergency response, disaster warnings, or
23 public health measures;
- 24 (2) Substantial and measurable economic harm, including large-scale fraud,
25 financial, or market manipulation; and
- 26 (3) Obstruction of critical public services or infrastructure, including
27 elections, emergency systems, utilities, or essential government
28 functions;
- 29 (aa) *VLP-PH* refers to a digital platform designated by the DICT as reaching
30 at least ten percent (10%) of the national population in average monthly active
31 users, or such other risk-based threshold and methodology as the DICT may
32 publish annually; and

1 (bb) *Vetted researchers* refer to third party academics, journalists, or civil society
2 organizations accredited by the DICT or the National Privacy Commission
3 (NPC) to access platform data for the purpose of studying systemic risks,
4 subject to strict privacy, cybersecurity, and confidentiality safeguards.
5

6 CHAPTER III 7 PROHIBITED ACTS 8

9 **SEC. 4. *Prohibited Acts.*** – It shall be unlawful for any natural or juridical person
10 to knowingly and willfully:

- 11 (a) Publish, disseminate, finance, direct, or materially assist in the dissemination
12 of false information, with actual knowledge of its falsity or reckless disregard for
13 its truth, and with specific intent to cause verifiable public harm or a serious
14 threat to national security;
- 15 (b) Operate, finance, direct, or materially assist a CIB network, troll farm, bot
16 network, fake account network, or deceptive digital operation intended to
17 deceive the public and cause verifiable public harm or a serious threat to
18 national security;
- 19 (c) Publish, or disseminate synthetic or materially manipulated media, without
20 adequate disclosure, with actual knowledge of its deceptive character and
21 specific intent to cause verifiable public harm or a serious threat to national
22 security;
- 23 (d) Act on behalf of, in coordination with, or under the substantial direction or
24 control of a foreign state, foreign intelligence service, foreign military actor, or
25 foreign-funded covert influence operation to disseminate disinformation that
26 poses a serious threat to national security; or
- 27 (e) Impersonate a government agency, election body, emergency-response
28 authority, public-health authority, court, law-enforcement agency, educational
29 institution, media organization, or real person for the purpose of disseminating
30 disinformation that causes verifiable public harm or a serious threat to national
31 security.

1 Mere liking, sharing, forwarding, or reposting without actual knowledge of falsity
2 and specific intent to cause verifiable public harm shall not be deemed dissemination
3 under this Act.

4
5 **SEC. 5. *Protection of Free Speech, Legitimate Expression, and Other Related***
6 ***Rights.*** – This Act shall not be construed to suppress protected expression, including
7 political opinions, criticism of government, criticism of public officials or candidates,
8 satire, journalistic inquiry, investigative reporting, editorial judgment, whistleblowing,
9 public interest advocacy, commentary, opinion, academic discourse, artistic and
10 religious expression, and other forms of protected speech. It shall also not be used to
11 penalize inadvertent errors made in good faith and subsequently corrected,
12 expressions clearly identified as humor or creative content, nor shall it target
13 individuals or groups engaging in legitimate political organizing or online advocacy.

14
15 **CHAPTER IV**
16 **DIGITAL PLATFORM ACCOUNTABILITY**

17
18 **SEC. 6. *Platform Obligations.*** – All digital platforms operating in the Philippines
19 shall:

- 20 (a) Establish and maintain a legal entity or permanent representative office in the
21 Philippines for compliance, coordination, regulatory and ethical accountability,
22 where they may be properly served with summons or notices by competent
23 Philippine authorities;
- 24 (b) Disclose publicly and in real time sponsored content, political advertisements,
25 and paid campaigns, and significant takedowns of networks or accounts
26 engaged in CIB;
- 27 (c) Submit annual transparency reports to the DICT detailing actions taken against
28 CIB, bot networks, and impersonation;
- 29 (d) Provide anonymized and aggregate data necessary for oversight, consistent
30 with Republic Act (R.A.) No. 10173 or the “Data Privacy Act of 2012,” R.A. No.
31 10175 or the “Cybercrime Prevention Act of 2012,” and internationally accepted
32 cybersecurity standards; any access beyond aggregate/anonymized data shall
33 require DICT pre-approval and, where personal or content data are involved,
34 judicial authorization;

- (e) Maintain an accessible Notice-and-Action mechanism for users to report allegedly unlawful content;
- (f) Provide an SoR to affected users for any restriction, suspension, or removal of content or accounts, stating the decision taken, the legal or policy basis, the facts relied upon, whether automation was used, and available redress. Anonymized SoRs shall be transmitted to a DICT Transparency Portal within twenty-four (24) hours;
- (g) Provide users with an internal complaint-handling system and access to certified ODS bodies under the DICT for unresolved disputes;
- (h) Maintain a searchable public ad repository that contains, at minimum, the ad creative, sponsor, payor, targeting criteria, spend, and dates of display;
- (i) Ensure that advertisements are not targeted at minors and are not targeted using sensitive personal information as defined by the Data Privacy Act of 2012;
- (j) Provide transparency on recommender systems and offer users a clearly accessible option to view content feeds not based on profiling; and
- (k) Refrain from deploying manipulative interface designs or “dark patterns” that materially distort or impair user autonomy, decision-making, or choice.

No digital platform, hosting provider, intermediary, officer, employee, or representative shall be held liable under this Act solely by reason of hosting, transmitting, indexing, ranking, recommending, or moderating third-party content, absent proof beyond reasonable doubt of knowing, active, and material participation in the prohibited conduct under Section 4 of this Act.

Failure to comply with platform obligations under this Act shall be subject only to administrative penalties, unless the platform or its responsible officers knowingly directed, financed, or materially participated in the prohibited conduct.

SEC. 7. Platform Obligations of VLP-PH. – VLP-PHs designated by the DICT, in addition to Section 6 of this Act shall:

- (a) Conduct and publish annual systemic risk assessments addressing, at minimum, disinformation, manipulation, civic discourse, protection of minors, public health emergencies, disaster response, and election integrity;

- 1 (b) Publish and implement proportionate risk-mitigation plans;
- 2 (c) Undergo an independent annual audit, filing full results with DICT and a public
3 summary;
- 4 (d) Appoint a senior compliance officer based in the Philippines responsible for
5 obligations under this Act;
- 6 (e) Provide vetted researchers, accredited by the NPC or the DICT, with secured
7 access to data necessary for studying system risks, subject to strict privacy
8 and cybersecurity standards;
- 9 (f) Designate a duly authorized liaison officer to the DICT, who shall serve as the
10 official point of contact of the platform on the following:
 - 11 (1) Compliance with this Act and other cyber-related laws;
 - 12 (2) Coordination on takedown or moderation requests involving malicious
13 disinformation that threatens national security or public order;
 - 14 (3) Emergency responses during critical events such as elections, disasters,
15 or public health crises; and
 - 16 (4) Reporting obligations and transparency measures as may be required
17 by the DICT or Congress.
- 18 (g) Publish and enforce transparent policies and procedures designed to mitigate
19 the risks posed by CIB, impersonation, bot networks, manipulated media,
20 concealed sponsorship, and the algorithmic amplification of content
21 determined through established review mechanisms. Platforms may employ
22 proportionate visibility-reduction measures, contextual labeling, fact-check
23 notices, and algorithmic de-amplification for content determined through
24 established review mechanisms to be demonstrably and likely to cause
25 verifiable public harm or seriously threaten national security;
- 26 (h) Maintain publicly accessible page and advertising transparency, including
27 sponsor identification and ad placement disclosures; and
- 28 (i) Engage with independent third-party fact-checking organizations in providing
29 context, labeling, or verification, and with academic, professional, and civil
30 society organizations, to promote media and information literacy.

1 **SEC. 8. *Data Access and Technical Cooperation.*** – In connection with Section
2 7(c) and (e), platforms shall provide reasonable technical cooperation, including
3 access to application programming interfaces (APIs), metadata, and transparency
4 dashboards, to support oversight and audits, subject to privacy and cybersecurity
5 safeguards.

6
7 **CHAPTER V**
8 **PENALTIES**

9 **SEC. 9. *Penalties.*** – Any person found guilty of violating Section 4 of this Act
10 shall suffer the penalty of imprisonment of six (6) years to twelve (12) years and a fine
11 of not less than Five hundred thousand pesos (P500,000) but not more than Two
12 million pesos (P2,000,000), or both, at the discretion of the court.

13 **SEC. 10. *Penalties for Non-Compliance by Platforms.*** – After due notice and
14 hearing, any platform that, without lawful excuse, fails or refuses to comply with
15 obligations under Sections 6, 7, and 8, shall be subjected to the following penalties:

- 16 (a) First offense - written warning and compliance order from the DICT; and
17 (b) Second and subsequent offenses – penalty of not less than One million
18 pesos (P1,000,000) but not more than Ten million pesos (P10,000,000),
19 depending on the gravity of the offense.

20 For VLP-PHs, the DICT may additionally impose an administrative penalty
21 of up to six percent (6%) of Philippine annual gross revenue for repeated
22 violations.

23
24 The DICT shall publish an annual list of non-compliant platforms for public
25 transparency.

26 **SEC. 11. *Transition Period.*** – Platforms shall have a two-year transition period
27 from effectivity of this Act to fully comply with reporting, ad repository, and systemic-
28 risk audit obligations. The DICT may phase requirements by platform size and risk.

CHAPTER VI
JURISDICTION AND OVERSIGHT

SEC. 12. *Judicial Recourse and Appeal.* –

(a) The Regional Trial Courts shall have jurisdiction over any violation of the provisions of this Act regardless of the place of commission. A Filipino national who commits any of the offenses defined under Section 4 of this Act shall be within the jurisdiction of the Philippine courts. The venue shall be the residence of the accused; and

(b) The Commission on Human Rights may provide legal and monitoring assistance in cases involving allegations of abuse of this Act for political or retaliatory purposes.

SEC. 13. *Enforcement.* – The cybercrime units of relevant agencies shall investigate and prosecute prohibited conduct under Section 4 of this Act. The DICT shall oversee platform compliance with the obligations set out in Sections 6, 7, and 8 of this Act.

SEC. 14. *Relation to Existing Laws.* – The Cybercrime Prevention Act of 2012 shall apply suppletory only to cybercrime procedure, preservation, disclosure, jurisdiction, and law-enforcement coordination, subject to constitutional limitations and judicial authorization. Nothing in this Act shall authorize double prosecution or double punishment for the same act, nor revive provisions of the Cybercrime Prevention Act of 2012 previously declared unconstitutional. Prosecution under this Act shall bar any other prosecution arising from the same Acts.

CHAPTER VII
MEDIA AND DIGITAL LITERACY

SEC. 15. *Promotion of Media and Digital Literacy.* – The Department of Education (DepEd) and the Commission on Higher Education (CHED), in partnership with civil society, shall integrate media and digital literacy into curricula at all levels. Such programs shall emphasize critical thinking, fact-checking, responsible online behavior, and verification of information and images. Teacher training, public modules, and assessment systems shall be developed in consultation with civil society, the academe, and media organizations to ensure proper implementation.

1 **SEC. 16. *Government Communication Standards.*** – All national government
2 agencies, and, where feasible, local government units, shall maintain open data
3 portals containing verifiable public information. They shall also correct erroneous or
4 misleading public statements within a reasonable time upon discovery, indicating the
5 nature of the error and the source of the verified information.

6 **CHAPTER VIII**
7 **FINAL PROVISIONS**
8

9 **SEC. 17. *Joint Congressional Oversight Committee (JCOC).*** – There shall be
10 created a Joint Congressional Oversight Committee which shall monitor and ensure
11 the effective implementation of this Act. It shall determine weaknesses and loopholes
12 in the law, recommend the necessary remedial legislation or administrative measures
13 and perform such other duties and functions as may be necessary to attain the
14 objectives of this Act.

15 The JCOC shall be composed of five (5) Members from the Senate and five (5)
16 Members from the House of Representatives with the Chairperson of the Committee
17 on Public Information and Mass Media of the Senate, and the Chairpersons of the
18 Committees on Public Information and Information and Communications Technology
19 of the House of Representatives as Co-Chairpersons of the JCOC: *Provided*, That one
20 (1) Member from each chamber shall come from the minority party or bloc.

21 **SEC. 18. *Sunset Review.*** – Within two (2) years after the effectivity of this Act,
22 or as the need arises, the JCOC shall conduct a sunset review. For purposes of this
23 Act, the term "sunset review" shall mean a systematic evaluation by the JCOC of the
24 accomplishments and impact of this Act, as well as the performance of the agencies
25 responsible for its implementation, for purposes of determining remedial legislation.

26 **SEC. 19. *Implementing Rules and Regulations.*** – Within ninety (90) days from
27 the effectivity of this Act, the DICT shall, in consultation with relevant government
28 agencies, the private sector and civil society organizations, promulgate the
29 implementing rules and regulations for the effective implementation of this Act.

1 **SEC. 20. *Separability Clause.*** – If any section or part of this Act is held
2 unconstitutional or invalid, the other sections or provisions not otherwise affected shall
3 remain in full force and effect.

4 **SEC. 21. *Repealing Clause.*** – All laws, decrees, executive order, rules and
5 regulations, issuances, or any part thereof inconsistent with the provisions of this Act
6 are deemed repealed.

7 **SEC. 22. *Effectivity.*** – This Act shall take effect fifteen (15) days after its
8 publication in the *Official Gazette* or in a newspaper of general circulation.

Approved,