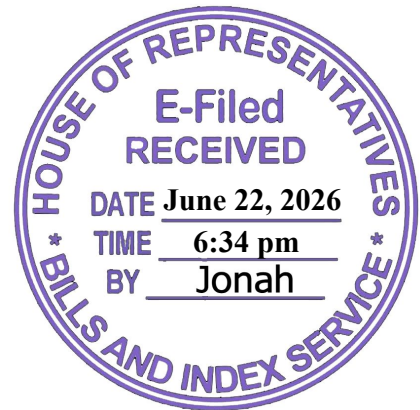




Republic of the Philippines
House of Representatives
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL No. 9907



Introduced by **HONORABLE ERNESTO “ERNIX” M. DIONISIO, JR.**

**AN ACT AMENDING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE
“CYBERCRIME PREVENTION ACT OF 2012,” TO CRIMINALIZE THE
UNAUTHORIZED AND MALICIOUS USE OF ARTIFICIAL INTELLIGENCE
SYSTEMS FOR IDENTITY THEFT, ONLINE FRAUD, COMPUTER-RELATED
FORGERY, AND OTHER COMPUTER-RELATED OFFENSES, PROVIDING
SAFEGUARDS FOR LEGITIMATE USES, AND FOR OTHER PURPOSES**

EXPLANATORY NOTE

The rapid advancement and widespread accessibility of Artificial Intelligence (AI) technologies have transformed the digital landscape, creating unprecedented opportunities for innovation, economic growth, and public service. However, the same technologies have also introduced new avenues for cybercrime, particularly through the creation of highly realistic synthetic identities, deepfakes, voice cloning, automated impersonation schemes, and other AI-generated content capable of deceiving individuals, businesses, and government institutions.

Republic Act No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012," penalizes computer-related identity theft, fraud, forgery, and related cyber offenses. Nevertheless, the law was enacted before the emergence of modern generative artificial intelligence systems, and does not expressly address the unique risks posed by AI-enabled criminal activities.

Recent developments have demonstrated how AI can be exploited to impersonate individuals through fabricated images, cloned voices, manipulated videos, and synthetic digital identities. Such technologies have been used to facilitate financial scams, phishing schemes, identity theft, reputational attacks, misinformation campaigns, and other fraudulent activities. The increasing sophistication of these tools has made it more difficult for victims, law enforcement authorities, and the public to distinguish authentic content from fabricated material.

The absence of explicit statutory provisions governing AI-assisted cybercrime creates uncertainty in enforcement and may limit the ability of authorities to effectively

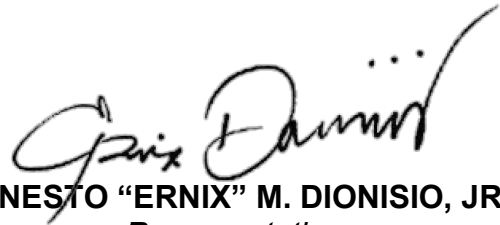
investigate and prosecute offenders who use emerging technologies as instruments of criminal activity. While existing provisions of Republic Act No. 10175 may apply in certain instances, there is a compelling need to clearly define and penalize the unauthorized use of artificial intelligence systems for identity theft, online fraud, computer-related forgery, and other cyber offenses.

This proposed measure seeks to amend Republic Act No. 10175 by:

- (1) Defining artificial intelligence systems, synthetic identities, and deepfakes for purposes of criminal liability;
- (2) Criminalizing the unauthorized use of AI technologies to impersonate, deceive, or misrepresent the identity of natural or juridical persons;
- (3) Penalizing AI-assisted computer-related fraud and computer-related forgery;
- (4) Establishing the malicious deployment of AI systems for cybercriminal purposes as a punishable offense;
- (5) Treating the use of artificial intelligence as a qualifying circumstance that warrants higher penalties when employed in the commission of cybercrimes; and
- (6) Strengthening the capacity of law enforcement agencies to address emerging forms of technology-facilitated criminal conduct.

This bill does not seek to hinder legitimate research, innovation, or beneficial uses of artificial intelligence. Rather, it aims to promote the responsible and ethical use of AI technologies while safeguarding individuals, businesses, and public institutions from deception, fraud, and other harms arising from the malicious exploitation of these tools.

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



ERNESTO "ERNIX" M. DIONISIO, JR.
Representative
First District, City of Manila



Republic of the Philippines
House of Representatives
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL No. 9907

Introduced by **HONORABLE ERNESTO “ERNIX” M. DIONISIO, JR.**

**AN ACT AMENDING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE
“CYBERCRIME PREVENTION ACT OF 2012,” TO CRIMINALIZE THE
UNAUTHORIZED AND MALICIOUS USE OF ARTIFICIAL INTELLIGENCE
SYSTEMS FOR IDENTITY THEFT, ONLINE FRAUD, COMPUTER-RELATED
FORGERY, AND OTHER COMPUTER-RELATED OFFENSES, PROVIDING
SAFEGUARDS FOR LEGITIMATE USES, AND FOR OTHER PURPOSES**

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

Section 1. Declaration of Policy. – It is hereby declared the policy of the State to protect individuals, businesses, and government institutions from cybercrimes facilitated through artificial intelligence systems. The State recognizes the benefits of artificial intelligence while ensuring that its development and use do not undermine privacy, security, public trust, and the integrity of digital communications and transactions.

Section 2. Definition of Terms. – A new subsection is hereby inserted under Section 3 of Republic Act No. 10175 to read as follows:

"(q) Artificial Intelligence (AI) System – refers to any machine-based system that, for explicit or implicit objectives, infers from inputs how to generate outputs such as predictions, content, recommendations, decisions, synthetic media, voice simulations, images, videos, or other digital outputs capable of influencing physical or virtual environments.

(r) Synthetic Identity – refers to an identity, profile, image, voice, likeness, biometric characteristic, or combination thereof that is wholly or partially generated, modified, replicated, or simulated through an AI system.

(s) Deepfake – refers to AI-generated or AI-manipulated audio, video, image, or digital representation that falsely appears authentic and depicts an identifiable person engaging in speech, conduct, or activities that did not occur.

(t) AI-Generated Content Disclosure - refers to a visible or invisible watermark, label, metadata tag, or other technological means that clearly indicates that content is AI-generated or AI-altered."

Section 3. Creation of New Offenses. – Section 4(b) of Republic Act No. 10175 is hereby amended by adding the following provisions:

"(4) AI-Assisted Identity Theft. – The intentional creation, generation, acquisition, use, transfer, possession, publication, dissemination, sale, or distribution of a synthetic identity or deepfake of another person, whether natural or juridical, without lawful authority or consent, for the purpose of deception, impersonation, fraud, harassment, extortion, financial gain, reputational harm, or the commission of any crime.

(5) AI-Assisted Computer-Related Fraud. – The use of an AI system to deceive, manipulate, impersonate, or induce any person, entity, or computer system into transferring money, property, credentials, access rights, confidential information, or any valuable consideration.

(6) AI-Assisted Computer-Related Forgery. – The generation, alteration, manipulation, or use of AI-generated content intended to be presented as authentic evidence, records, communications, instructions, or representations for legal, financial, commercial, governmental, or fraudulent purposes.

(7) Malicious Deployment of AI Systems. – The development, deployment, operation, sale, distribution, or provision of AI systems primarily designed or adapted for committing cybercrime offenses under this Act.

(8) Failure to Disclose AI-Generated Content. - Any person who publishes, disseminates, or distributes AI-generated or AI-manipulated audio, video, or image depicting an identifiable person without a clear and conspicuous AI-Generated Content Disclosure, when such omission is intended to deceive, mislead, or cause harm."

Section 4. Exceptions and Protected Uses. – A new section is hereby inserted after Section 4 of Republic Act No. 10175:

"Section 4-A. Exceptions.

The Provisions of Sections 4(b)(4) and 4(b)(6) shall not apply to:

1. **Content created with the express consent** of the person depicted;
2. **Satire, parody, caricature, artistic expression, or commentary**, provided there is no intent to defraud, extort, or cause harm;
3. **Journalistic, academic, scientific, or research activities**, including cybersecurity testing, conducted in good faith and without intent to deceive or commit a crime;
4. **AI-generated content that does not depict a real, identifiable person**;
5. **Content containing proper AI-Generated Content Disclosure**, where no malicious intent is present.

These exceptions shall not apply where the AI-generated content is used to commit fraud, extortion, identity theft, harassment, or any criminal act.”

Section 5. Qualifying Circumstances. – A new section is hereby inserted after Section 6 of Republic Act No. 10175:

"Section 6-A. AI as a Qualifying Circumstance. – When any offense punishable under this Act is committed through the use of an artificial intelligence system, deepfake technology, synthetic identity, automated decision-making system, or similar emerging technology, the penalty imposed shall be one (1) degree higher than that prescribed for the underlying offense."

Section 6. Mandatory Watermarking and Disclosure. – A new section is hereby inserted after Section 6-A of Republic Act No. 10175:

“Section 6-B. Mandatory Disclosure of AI-Generated Content. – Any AI-generated or AI-manipulated audio, video, or image depicting an identifiable person shall contain a clear and conspicuous watermark, label, metadata tag, or other disclosure indicating that the content is AI-generated or AI-altered.

Failure to include such disclosure shall constitute prima facie evidence of intent to deceive for purposes of prosecution under this Act.”

Section 7. Penalties. – Any person found guilty of offenses under Section 4(b)(4), 4(b)(5), 4(b)(6), or 4(b)(7), or 4(b)(8) shall suffer the penalty of *prision mayor* and a fine ranging from Five Hundred Thousand Pesos (₱500,000.00) to Five Million Pesos (₱5,000,000.00), without prejudice to prosecution under other applicable laws.

Section 8. Corporate Liability. – Where the offender is a corporation, partnership, association, or juridical entity, the responsible officers, directors,

managers, or employees who knowingly authorized, directed, tolerated, or failed to prevent the commission of the offense shall be held criminally liable.

Section 9. Extraterritorial Application. – The provisions of this Act shall apply where the victim is a Filipino citizen, resident, business entity, or government agency, regardless of the location of the offender or the AI infrastructure used.

Section 10. Implementing Rules and Regulations. – Within ninety (90) days from the effectivity of this Act, the Department of Justice, the Department of Information and Communications Technology, the Cybercrime Investigation and Coordinating Center, the National Privacy Commission, and other relevant agencies shall promulgate the necessary rules and regulations for its implementation.

Section 11. Separability Clause. – If any portion or provision of this Act is declared unconstitutional, the remainder of this Act or any provisions not affected thereby shall remain in force and effect.

Section 12. Repealing Clause. – Any law, presidential decree or issuance, executive order, letter of instruction, rule or regulation inconsistent with the provisions of this Act is hereby repealed or modified accordingly.

Section 13. Effectivity. – This Act shall take effect fifteen (15) days following its complete publication in a newspaper of general circulation.

Approved,