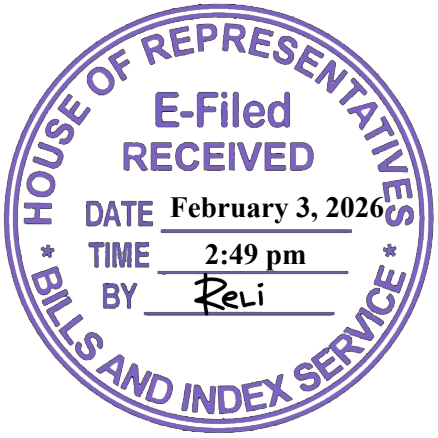
TWENTIETH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)



HOUSE BILL NO. 7584

Introduced by Representative JAIME EDUARDO MARC D. COJUANGCO

EXPLANATORY NOTE

In recognition of the increasing capabilities of artificial intelligence (AI) and its potential to manipulate and misuse the voices and faces of individuals, including public figures, it is imperative to establish legal safeguards to protect the integrity and privacy of individuals' identities.

This bill aims to regulate the unauthorized use of AI-generated voice and facial simulations for malicious purposes, including but not limited to deceptive audio, visual media ('*Deepfakes*'), and misinformation.

This enactment is a measure to protect the identity and reputation of persons in this age of technological advancements.

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

JAIME EDUARDO MARC D. COJUANGCO
Representative
1st District of Tarlac

TWENTIETH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)

HOUSE BILL NO. 7584

Introduced by Representative JAIME EDUARDO MARC D. COJUANGCO

AN ACT
PROTECTING THE VOCAL AND FACIAL IDENTITY OF PERSONS AGAINST VIRTUAL IMPERSONATION AND DEEPFAKE RECORDINGS AND IMAGES

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

Section 1. ***Title.*** – This Act shall be known as the "Protection of Voice and Facial Identity Act".

Section 2. ***Declaration of Policy.*** – The State recognizes the essential role of science and technology for national development and progress such as content creation, data processing, broadcasting electronic commerce, in the nation's social and economic progress. The State also acknowledges the significance of regulating the use of technology and the necessity of protecting and safeguarding the identities of persons in relation to the use of computer related programs. In this light, the State shall enact means to protect the identity of persons against misuse of Artificial Intelligence generated voice and facial simulations.

Section 3. ***Definition of Terms.*** – For purposes of this Act, the following terms are hereby defined as follows:

(a) *Artificial Intelligence* (AI) refers to a machine or software that has the capacity to mimic human cognitive functions, including, but not limited to, learning, problem solving, and pattern recognition, which enables the machine or software to perform tasks that normally require human intelligence. AI includes various subfields,

including, but not limited to, machine learning, natural language processing, and large language models.

(b) *Voice Simulation* refers to the replication or synthesis of an individual's voice using AI technology.

(c) *Facial Simulation* refers to the replication or synthesis of an individual's facial features and expressions using AI technology.

(d) *Public Figure* refers to any individual who holds a position of public prominence or influence, including but not limited to politicians, celebrities, and other recognizable personalities.

(e) *Without consent* refers to the conduct undertaken without any consent from the person whose vocal and/or facial identity is being used.

(f) *Deepfake impersonation a*ny audio or visual media in an electronic format, including any motion picture film or video recording, that is created or altered in a manner that it would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of the individual depicted in the recording.

As used in this section, "deepfake" does not include any material that constitutes a work of political, public interest, or newsworthy value, including commentary, criticism, satire, or entertainment, or that includes content, context, or a clear disclosure visible throughout the duration of the recording that would cause a reasonable person to understand that the audio or visual media is not a record of a real event.

Section 4. ***Punishable Acts.*** - The following acts constitute the offense of deepfake impersonation punishable under this Act:

(a) It shall be unlawful for any person, entity, or organization to create an AI-generated voice or facial simulations or deepfake impersonation using a person's name, voice, signature, photograph, video or likeness, in any manner, including public figures, *without consent* from the person being depicted in the deepfake.

(b) It shall also be unlawful for any person, entity, or organization to use and/or disseminate an AI-generated voice or facial simulations or deepfake impersonation using a person's name, voice, signature, photograph, video or likeness, in any manner, of another person, including public figures, with intent to defraud other persons or with intent to harass other persons.

Section 5. ***Exceptions.*** – Entertainment, parody, artistic expression, research, education, criticism or circumstances where it is clear to a reasonable listener or viewer that the recording, image or video has been digitally manipulated or simulated are not fraudulent.

If a person creates an image or video that uses artificial intelligence to mimic or replicate another person's voice or likeness in a manner that would otherwise deceive an average viewer, and displays the content for public viewing, the creator must provide a disclosure on the bottom of the image or video that the image or video is not authentic and does not reflect the original voice or likeness of the person being depicted, unless the person whose voice or likeness is being depicted consents to its use.

Section 6. ***Liability under Other Laws***. — A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.

Section 7. Penalties. — Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of prision mayor or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to a maximum amount commensurate to the damage incurred or both.

Section 8. ***Corporate Liability.*** — When any of the punishable acts herein defined are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on: (a) a power of representation of the juridical person provided the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person: *Provided,* That the act committed falls within the scope of such authority; or (c) an authority to exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten million pesos (PhP10,000,000.00).

If the commission of any of the punishable acts herein defined was made possible due to the lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Five million pesos (PhP5,000,000.00).

The liability imposed on the juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.

Section 9. ***Enforcement and Implementation*****.** – The Department of Information and Communication Technology (DICT), Department of Justice (DOJ), and the Cybercrime Unit of the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act.

The DICT shall also be responsible for raising public awareness about the risks associated with AI-generated content and promoting best practices for its ethical use.

Section 10. ***Traffic and Computer Data***. – The collection of real-time traffic data, the preservation, disclosure, search, seizure, examination, custody, destruction, restriction or blocking access to, of the computer data, shall be governed by Sections 11, 12, 13, 14, 15, 16, 17, 18, 19, and 20 of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012.

Section 11. ***Jurisdiction.*** — The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act. including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

Section 12. ***Implementing Rules and Regulations.*** – The DOST, the DOJ and the Department of the Interior and Local Government (DILG) shall jointly formulate the necessary rules and regulations within ninety (90) days from approval of this Act, for its effective implementation.

Section 13. ***Separability Clause.*** — If any provision or portion of this Act is subsequently declared unconstitutional, the remainder of this Act or any provision not thereby affected shall remain in full force and effect.

Section 14. ***Effectivity*****.** – This Act shall take effect fifteen (15) days after its complete publication in at least two (2) newspapers of general circulation in the Philippines.

Approved,