



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 10308



Introduced by Representative CARLOS A. LORIA

EXPLANATORY NOTE

Presidential Decree No. 1727, otherwise known as the “Anti-Bomb Joke Law,” was enacted on 08 October 1980 to penalize the malicious dissemination of false information and the willful making of threats concerning bombs, explosives, or similar devices. More than four decades since its enactment, the law has remained unchanged despite the profound transformation of the means by which such threats are now perpetrated.

The recent series of fake bomb threats in Masbate City and Camarines Norte, many of which were propagated through mobile phones, social media, and other online platforms, have exposed the inadequacy of a law that was crafted in an era before the advent of modern information and communications technology (ICT). As correctly pointed out by the Police Regional Office 5 of the Philippine National Police, PD 1727 did not anticipate ICT-enabled threats and, as such, provides no mechanism for the swift preservation of digital evidence, the expedited issuance of cyber warrants, or the imposition of penalties commensurate to the scale of disruption that a single, anonymously posted online bomb threat can now cause — from the suspension of classes and government operations, to evacuations, stampedes, and substantial economic losses.

This bill, drawn from the recommendations of the Technical Working Group of PRO 5, seeks to modernize PD 1727 by: (a) classifying ICT-enabled bomb threats as a cybercrime offense punishable under Republic Act No. 10175; (b) imposing higher penalties when a bomb threat results in aggravating circumstances such as suspension of classes or business operations, evacuation and damage to critical infrastructure, injury or death due to stampede, public chaos arising from social media posts, or substantial public alarm and economic loss; (c) requiring the immediate preservation of digital evidence by telecommunications and internet service providers; (d) streamlining the procedure for the issuance of cyber warrants in emergency bomb threat cases; (e) mandating the cooperation of local and foreign-based service providers; (f) institutionalizing a standardized regional inter-agency bomb threat response framework; and (g) intensifying public awareness and deterrence campaigns.

Bomb threats, whether uttered in person or posted online, are not harmless pranks. They endanger lives, disrupt the delivery of basic services, and inflict real economic damage on our communities. It is time that our laws catch up with the technology being used to commit this offense.

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


CARLOS A. LORIA
2nd District, Albay



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 10308

Introduced by Representative CARLOS A. LORIA

AN ACT AMENDING PRESIDENTIAL DECREE NO. 1727, OTHERWISE KNOWN AS THE "ANTI-BOMB JOKE LAW," CLASSIFYING BOMB THREATS COMMITTED THROUGH INFORMATION AND COMMUNICATIONS TECHNOLOGY AS A CYBERCRIME OFFENSE, IMPOSING STIFFER PENALTIES, PROVIDING FOR THE PRESERVATION OF DIGITAL EVIDENCE AND EXPEDITED CYBER WARRANT PROCEDURES, MANDATING THE COOPERATION OF SERVICE PROVIDERS, INSTITUTIONALIZING A BOMB THREAT RESPONSE FRAMEWORK, 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 "Anti-Bomb Joke Law of 1980, as Amended".

SEC. 2. Declaration of Policy. — It is the policy of the State to protect public safety and security, and to ensure the uninterrupted delivery of basic services, by penalizing the malicious dissemination of false information and the willful making of threats concerning bombs, explosives, or similar devices, whether committed in person or through the use of information and communications technology (ICT). Towards this end, the State shall adopt modern, technology-responsive measures, including the preservation of digital evidence and the expedited issuance of cyber warrants, to ensure the swift identification, apprehension, and prosecution of offenders.

SEC. 3. Section 1 of Presidential Decree No. 1727 is hereby amended to read as follows:

"SECTION 1. Any person who, by word of mouth or through the use of the mail, telephone, telegraph, printed materials, information and communications technology (ICT), including but not limited to the internet, mobile applications, text messaging, and social media or other online platforms, or other instrument or means of communication, willfully makes any threat or maliciously conveys, communicates, transmits, imparts, passes on, publishes, or otherwise disseminates false information, knowing the same to be false, concerning an attempt or alleged attempt being made to kill, injure, or intimidate any individual, or unlawfully to damage or destroy any building, vehicle, or other real or personal property, by means of explosives, incendiary devices, and other destructive forces of similar nature or characteristics, shall upon conviction be punished with imprisonment of not more than five (5) years, or a fine of not more than Two Hundred Thousand Pesos (P200,000.00), or both, at the discretion of the court having jurisdiction over the offense herein defined and penalized: Provided, That when the threat penalized under this Section is committed through the use of ICT, the offender shall likewise be held liable for a cybercrime offense under Republic Act No. 10175, otherwise known as the 'Cybercrime Prevention Act of 2012,' without prejudice to the penalty imposable under said Act."

SEC. 4. A new section is hereby inserted after Section 1 of Presidential Decree No. 1727, to be known as Section 1-A, to read as follows:

“SECTION 1-A. Aggravating Circumstances; Higher Penalties. — The penalty of imprisonment of six (6) years and one (1) day to twelve (12) years, and a fine of not less than Two Hundred Thousand Pesos (P200,000.00) but not more than One Million Pesos (P1,000,000.00), both at the discretion of the court, shall be imposed if the threat penalized under Section 1 hereof results in any of the following:

- (a) the suspension of classes, work, or disruption of government or private business operations;
- (b) the evacuation of facilities and personnel, or damage to critical infrastructure;
- (c) injury, death, or loss of limb of any person resulting from a stampede or panic caused by the threat;
- (d) chaos or public turmoil arising from the posting of the threat on social media or other online platforms; or
- (e) substantial public alarm and economic losses.

If the threat results in the death of any person, the penalty of reclusion temporal shall be imposed, without prejudice to the offender's liability for such other crimes as may have been committed.”

SEC. 5. A new section is hereby inserted, to be known as Section 1-B, to read as follows:

“SECTION 1-B. Preservation of Digital Evidence. — Upon receipt of a request from law enforcement authorities investigating a violation of this Act, telecommunications companies, internet service providers, and other online service providers shall immediately preserve the integrity of subscriber information, traffic data, and content data relevant to the investigation for a minimum period of ninety (90) days, which period may be extended for another ninety (90) days upon a renewed request, pending the issuance of the appropriate warrant under the Rule on Cybercrime Warrants and Republic Act No. 10175.”

SEC. 6. A new section is hereby inserted, to be known as Section 1-C, to read as follows:

“SECTION 1-C. Expedited Issuance of Cyber Warrants in Emergency Cases. — In cases involving an imminent threat to public safety, law enforcement authorities may apply for the expedited issuance of a Warrant to Disclose Computer Data, Warrant to Intercept Computer Data, or such other warrant as may be necessary under the Rule on Cybercrime Warrants, and the designated cybercrime court shall act on the application within twenty-four (24) hours from receipt thereof.”

SEC. 7. A new section is hereby inserted, to be known as Section 1-D, to read as follows:

“SECTION 1-D. Mandatory Cooperation of Service Providers. — All local and foreign-based telecommunications companies, internet service providers, and other online service providers doing business in the Philippines shall extend full cooperation and comply with lawful orders issued by competent authorities in connection with the investigation and prosecution of offenses under this Act, subject to existing laws, Republic Act No. 10175, and applicable international cooperation frameworks. Willful refusal or unjustified failure to comply with a lawful order under this Section shall be punishable under Republic Act No. 10175 and other applicable laws.”

SEC. 8. A new section is hereby inserted, to be known as Section 1-E, to read as follows:

“SECTION 1-E. Regional Bomb Threat Response Framework. — The Philippine National Police, in coordination with the Department of Information and Communications Technology, the Department of Education, the Commission on Higher Education, concerned local government units, telecommunications and internet service providers, and other emergency response organizations, shall establish a standardized inter-agency protocol for the timely reporting, threat assessment, investigation, and prosecution of bomb threat incidents, whether committed physically or through the use of ICT.”

SEC. 9. A new section is hereby inserted, to be known as Section 1-F, to read as follows:

“SECTION 1-F. Public Awareness and Deterrence Campaign. — The Philippine National Police, in coordination with the Department of Information and Communications Technology and other concerned agencies, shall conduct a continuing public information campaign emphasizing that bomb threats, whether committed physically or through online platforms, are serious criminal offenses carrying substantial penalties under this Act and Republic Act No. 10175, and may result in criminal prosecution under both laws.”

SEC. 10. Section 2 of Presidential Decree No. 1727 is hereby amended to read as follows:

“SECTION 2. Jurisdiction. — All cases arising from a violation of this Act shall be filed with, and tried by, the Regional Trial Court of the place where the offense, or any of its essential elements, was committed or, if the offense was committed through the use of information and communications technology, by the Regional Trial Court designated as a cybercrime court pursuant to Republic Act No. 10175, which shall have original jurisdiction over the same. The accused shall be entitled to bail as a matter of right or discretion, in accordance with the Rules of Court and existing law.”

SEC. 11. Implementing Rules and Regulations. — Within ninety (90) days from the effectivity of this Act, the Philippine National Police, in coordination with the Department of Justice, the Department of Information and Communications Technology, the National Telecommunications Commission, and other concerned agencies, shall promulgate the necessary rules and regulations to implement the provisions of this Act.

SEC. 12. Separability Clause. — If any provision of this Act is declared unconstitutional or invalid, the other provisions not affected thereby shall remain in full force and effect.

SEC. 13. Repealing Clause. — All laws, decrees, executive orders, rules and regulations, or parts thereof, inconsistent with the provisions of this Act are hereby repealed, amended, or modified accordingly.

SEC. 14. Effectivity. — This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,