[DOJ RULES AND REGULATIONS IMPLEMENTING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE "CYBERCRIME PREVENTION ACT OF 2012", August 12, 2015]

DOJ RULES AND REGULATIONS IMPLEMENTING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE "CYBERCRIME PREVENTION ACT OF 2012"

Adopted: 12 August 2015
Date Filed: 21 September 2015

Pursuant to the authority of the Department of Justice, Department of Interior and Local Government, and Department of Science and Technology under Republic Act No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012", the following rules and regulations are hereby promulgated to implement the provisions of said Act:

RULE 1
Preliminary Provisions

Section 1. *Title*. – These Rules shall be referred to as the Implementing Rules and Regulations of Republic Act No. 10175, or the "Cybercrime Prevention Act of 2012".

Section 2. *Declaration of Policy*. – The State recognizes the vital role of information and communications industries, such as content production, telecommunications, broadcasting, electronic commerce and data processing, in the State's overall social and economic development.

The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks and databases, and the confidentiality, integrity, and availability of information and data stored therein from all forms of misuse, abuse and illegal access by making punishable under the law such conduct or conducts.

The State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

Section 3. *Definition of Terms*. – The following terms are defined as follows:

a) ***Access*** refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network;
b) ***Act*** refers to Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012";
c) ***Alteration*** refers to the modification or change, in form or substance, of an existing computer data or program;
d) ***Central Authority*** refers to the DOJ – Office of Cybercrime;
e) ***Child Pornography*** refers to the unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009", committed through a computer system: Provided, that the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775;
f) ***Collection*** refers to gathering and receiving information;
g) ***Communication*** refers to the transmission of information through information and communication technology (ICT) media, including voice, video and other forms of data;
h) ***Competent Authority*** refers to either the Cybercrime Investigation and Coordinating Center or the DOJ – Office of Cybercrime, as the case may be;
i) ***Computer*** refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing or storage functions, and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device, including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet;
j) ***Computer data*** refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function, and includes electronic documents and/or electronic data messages whether stored in local computer systems or online;
k) ***Computer program*** refers to a set of instructions executed by the computer to achieve intended results;
l) ***Computer system*** refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities, including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components, which may stand alone or be connected to a network or other similar devices. It also includes computer data storage devices or media;
m) ***Content Data*** refers to the communication content of the communication, the meaning or purport of the communication, or the message or information being conveyed by the communication, other than traffic data.
n) ***Critical infrastructure*** refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data that are so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters;

o) ***Cybersecurity*** refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, and organization and user's assets;
p) ***National Cybersecurity Plan*** refers to a comprehensive plan of actions designed to improve the security and enhance cyber resilience of infrastructures and services. It is a top-down approach to cybersecurity that contains broad policy statements and establishes a set of national objectives and priorities that should be achieved within a specific timeframe;
q) ***Cybersex*** refers to the willful engagement, maintenance, control or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration;
r) ***Cyber*** refers to a computer or a computer network, the electronic medium in which online communication takes place;
s) ***Database*** refers to a representation of information, knowledge, facts, concepts or instructions which are being prepared, processed or stored, or have been prepared, processed or stored in a formalized manner, and which are intended for use in a computer system;
t) ***Digital evidence*** refers to digital information that may be used as evidence in a case. The gathering of the digital information may be carried out by confiscation of the storage media (data carrier), the tapping or monitoring of network traffic, or the making of digital copies (e.g., forensic images, file copies, etc.), of the data held;
u) ***Electronic evidence*** refers to evidence, the use of which is sanctioned by existing rules of evidence, in ascertaining in a judicial proceeding, the truth respecting a matter of fact, which evidence is received, recorded, transmitted, stored, processed, retrieved or produced electronically;
v) ***Forensics*** refers to the application of investigative and analytical techniques that conform to evidentiary standards, and are used in, or appropriate for, a court of law or other legal context;
w) ***Forensic image***, also known as a ***forensic copy***, refers to an exact bit-by- bit copy of a data carrier, including slack, unallocated space and unused space. There are forensic tools available for making these images. Most tools produce information, like a hash value, to ensure the integrity of the image;
x) ***Hash value*** refers to the mathematical algorithm produced against digital information (a file, a physical disk or a logical disk) thereby creating a "digital fingerprint" or "digital DNA" for that information. It is a one-way algorithm and thus it is not possible to change digital evidence without changing the corresponding hash values;
y) ***Identifying information*** refers to any name or number that may be used alone or in conjunction with any other information to identify any specific individual, including any of the following:

    1. Name, date of birth, driver's license number, passport number or tax identification number;
    2. Unique biometric data, such as fingerprint or other unique physical representation;
    3. Unique electronic identification number, address or routing code; and
    4. Telecommunication identifying information or access device.

z) ***Information and communication technology system*** refers to system intended for, and capable of, generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording or storage of electronic data message or electronic document;

aa) ***Interception*** refers to listening to, recording, monitoring or surveillance of the content of communications, including procurement of the content of data, either directly through access and use of a computer system, or indirectly through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring;

bb) ***Internet content host*** refers to a person who hosts or who proposes to host internet content in the Philippines;

cc) ***Law enforcement authorities*** refers to the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) under Section 10 of the Act;

dd) ***Original author*** refers to the person who created or is the origin of the assailed electronic statement or post using a computer system;

ee) ***Preservation*** refers to the keeping of data that already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. It is the activity that keeps that stored data secure and safe;

ff) ***Service provider*** refers to:

1. any public or private entity that provides users of its service with the ability to communicate by means of a computer system; and
2. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

gg) ***Subscriber's information*** refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic or content data, and by which any of the following can be established:

1. The type of communication service used, the technical provisions taken thereto and the period of service;
2. The subscriber's identity, postal or geographic address, telephone and other access number, any assigned network address, billing and payment information that are available on the basis of the service agreement or arrangement; or
3. Any other available information on the site of the installation of communication equipment that is available on the basis of the service agreement or arrangement.

hh) ***Traffic Data or Non-Content Data*** refers to any computer data other than the content of the communication, including, but not limited to the communication's origin, destination, route, time, date, size, duration, or type of underlying service; and

ii) ***Without Right*** refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications or relevant principles under the law.

RULE 2
Punishable Acts and Penalties

Cybercrimes

Section 4. *Cybercrime Offenses*. – The following acts constitute the offense of core cybercrime punishable under the Act:

A. **Offenses against the confidentiality, integrity and availability of computer data and systems** prision mayor or a fine of at least Two Hundred Thousand Pesos (P200,000.00) up to a maximum amount commensurate to the damage incurred, or both, except with respect to number 5 herein:

1. **Illegal Access** – The access to the whole or any part of a computer system without right.
2. **Illegal Interception** – The interception made by technical means and without right, of any non-public transmission of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data: Provided, however, That it shall not be unlawful for an officer, employee, or agent of a service provider, whose facilities are used in the transmission of communications, to intercept, disclose or use that communication in the normal course of employment, while engaged in any activity that is necessary to the rendition of service or to the protection of the rights or property of the service provider, except that the latter shall not utilize service observing or random monitoring other than for purposes of mechanical or service control quality checks.
3. **Data Interference** – The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document or electronic data message, without right, including the introduction or transmission of viruses.
4. **System Interference** – The intentional alteration, or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document or electronic data message, without right or authority, including the introduction or transmission of viruses.
5. **Misuse of Devices**, which shall be punished with imprisonment of *prision mayor*, or a fine of not more than Five Hundred Thousand Pesos (P500,000.00), or both, is committed through any of the following acts:

    a. The use, production, sale, procurement, importation, distribution or otherwise making available, intentionally and without right, of any of the following:

        i. A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this rules; or