Adam Russel Shane P. Oguis

ITE185 – IT4D.1

Assignment 2

1. Read the Republic Act No. 10175 (Cybercrime Prevention Act of 2012) and discuss the following:

a. Discuss the overall context of the Cybercrime Prevention Act

-The Cybercrime Prevention Act of 2012 (RA 10175) is a Philippine law established to address legal issues relating to online interactions and the Internet. It was passed on September 12, 2012, and went into effect on February 27, 2014.

The overall goal of the Cybercrime Prevention Act is to safeguard individuals and organizations from cybercrime while also encouraging safe and responsible Internet use. The legislation defines and penalizes a wide range of cybercrimes, including:

- Illegal access to computer systems and data
- Data interference
- System interference
- Misuse of devices
- Cybersquatting
- Computer-related fraud
- Content-related offenses, such as cybersex and child pornography
- Other offenses, such as identity theft and online libel

b. Under this act, what are the categories that are considered as cybercrimes? Provide at least two (2) examples for each category

Violations of computer data and system confidentiality, integrity, and availability:

- Illegal access: Unauthorized access to a computer system or application.
- Illegal interception: Interception of any non-public communication of computer data to, from, or within a computer system.
- Data interference: is defined as the unauthorized acquisition, use, misuse, transfer, possession, alteration, or deletion of identifiable information belonging to another person, whether natural or juridical.

- System Interference: Intentional manipulation, damage, deletion, or destruction of computer data, programs, or systems
- Misuse of Devices: The use of any device to conduct any of the offenses listed in this Act.

Example:

* Breaking into a computer system in order to steal data

* Attempting to disrupt a computer system in order to launch a denial-of-service attack

* Disseminating malware in order to harm computers or steal data

Computer-related offenses:

- Computer-related fraud is defined as the unlawful modification, destruction, deletion, or change of computer data, programs, or systems.
- Computer-related forgery: The deliberate production or manipulation of computer data, programs, or systems to make them appear genuine, although knowing that they are fraudulent, inauthentic, or altered.
- Computer-related identity theft: the unlawful acquisition, use, misuse, transfer, possession, change, or deletion of identifying information belonging to another, whether natural or juridical, with the goal of gaining access to financial resources or impersonating another person.

Example:

* Using a phishing email to obtain someone's login information

* Setting up a bogus website to sell counterfeit goods

* Opening a credit card account with someone else's stolen Social Security number

Infractions involving content:

- Cybersex is defined as the purposeful involvement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual behavior via a computer system for favor or compensation.
- Child pornography is defined as any representation, through any means, of a child participating in actual or simulated explicit sexual activity, or any representation of a child's genital parts.

Example:

* Online distribution of child pornography

* Posting sexually explicit material involving a minor

c. What are the penalties for committing such punishable acts under this law?

- Illegal access: Imprisonment of six months to six years and a fine of not more than One hundred thousand pesos (Php100,000.00)
- Illegal interception: Imprisonment of one to seven years and a fine of not more than Two hundred thousand pesos (Php200,000.00)
- Data interference: Imprisonment of two to seven years and a fine of not more than Two hundred thousand pesos (Php200,000.00)
- System interference: Imprisonment of three to ten years and a fine of not more than Three hundred thousand pesos (Php300,000.00)
- Misuse of devices: Imprisonment of one to five years and a fine of not more than One hundred thousand pesos (Php100,000.00)
- Computer-related fraud: Imprisonment of two to seven years and a fine of not more than Two hundred thousand pesos (Php200,000.00)
- Computer-related forgery: Imprisonment of two to seven years and a fine of not more than Two hundred thousand pesos (Php200,000.00)
- Computer-related identity theft: Imprisonment of two to seven years and a fine of not more than Two hundred thousand pesos (Php200,000.00)
- Cybersex: Imprisonment of six to twelve years and a fine of not more than One million pesos (Php1,000,000.00)
- Child pornography: Imprisonment of six to twelve years and a fine of not more than One million pesos (Php1,000,000.00)

2. Read the GDPR (General Data Protection Regulation) of EU and the Data Privacy act of the Philippines and discuss the following:

a. Discuss the overall context of each law

GDPR (General Data Protection Regulation)

The GDPR is a data protection and privacy regulation under EU law that applies to the European Union (EU) and the European Economic Area (EEA). It also covers the transfer of personal data outside of the EU and EEA.

The GDPR's primary goal is to give citizens and residents back control over their personal data while also simplifying the regulatory environment for international business by unifying regulation inside the EU. It accomplishes this by repealing the 1995 Data Protection Directive (Directive 95/46/EC).

The GDPR governs the processing of personal data in the EU by both public and private organizations, as well as the transfer of personal data beyond the EU. It grants individuals several additional rights, including the right to access their personal data, the right to have their personal data erased, and the right to object to the processing of their personal data.

The GDPR also imposes new obligations on organizations that process personal data, such as obtaining consent from individuals before processing their personal data, implementing appropriate security measures to protect personal data, and reporting data breaches to the appropriate supervisory authority.

Data Privacy Act of the Philippines

The Data Privacy Act of the Philippines (DPA) is a law that preserves the fundamental human right to privacy while promoting innovation and growth by assuring the free flow of information. It allows for the free movement of personal data within the Union while respecting natural persons' fundamental rights and freedoms, including their right to personal data protection.

Within the extent of Union legislation, the DPA applies to the processing of personal data entirely or partially by automated means. It safeguards natural persons' fundamental rights and freedoms, including their right to personal data protection. Personal data must be handled fairly and legally.

The DPA compels enterprises to acquire individuals' consent before processing their personal data. It also requires enterprises to establish sufficient security measures to protect personal data and to notify the National Privacy Commission (NPC) of data breaches.

b. Discuss their similarities and differences. (Provide at least 2)

Similarities:

- Both laws aim to preserve individuals' personal data privacy.
- Both regulations require companies to seek individuals' consent before processing their personal data.

- Both regulations compel enterprises to use adequate security measures to safeguard personal information.
- Both regulations require enterprises to notify the appropriate authorities about data breaches.

Differences:

- The GDPR is broader in scope than the DPA and covers a broader range of activities.
- Individuals now have new rights under the GDPR, such as the right to have their personal data erased and the right to object to the processing of their personal data.
- The GDPR is more comprehensive than the DPA. The GDPR applies to all enterprises that process personal data of EU residents, regardless of where they are situated. The DPA, on the other hand, only applies to enterprises based in the Philippines or that process personal data of people residing in the Philippines.