UNDERSTANDING RA 10173 AND RA 10175

JULIAH JANE B. GEALON
IT IAS2: Information Assurance and Security 2

COR JESU COLLEGE, INC.
College of Computing and Information Sciences
Bachelor of Science in Information Technology

SEPTEMBER 18, 2025
DARYL IVAN H. HISOLA

Part A. RA 10173 – Data Privacy Act of 2012

1. **Differentiate between personal information, sensitive personal information, and privileged information. Give examples.**

Type of Information	Meaning	Examples
Personal Information	Basic details that identify a person.	Name, Age, Address, Phone Number, Email
Sensitive Personal Information	Private info that needs extra protection.	Password, Bank account numbers, Health records
Privileged Information	Shared in a trusted relationship, protected by law.	Doctor-patient records, Lawyer-client talks, counseling notes

2. **What is the role of the DPO in ensuring compliance with RA 10173?**
   - The Data Protection Officer (DPO) makes sure an organization follows the Data Privacy Act of 2012 (RA 10173). They create policies to protect personal data, train employees, and monitor compliance. The DPO also responds to data breaches, handles complaints, and coordinates with the National Privacy Commission (NPC). The DPO is the guardian of personal information in the organization.

3. **Explain at least two rights of data subjects with examples.**

   1. Right to be Informed - This means a person has the right to know how their personal data will be collected, used, stored, and shared.
   - **Example:** When you sign up for Shopee, it explains in its privacy policy how your name, address, and phone number will be used for deliveries.

   2. Right to Access - This means a person has the right to see or request a copy of the personal data that an organization has about them.
   - **Example:** If a student asks their school for a copy of their personal records (like grades or contact details kept in the system), the school must provide it.

4. **What penalties await organizations that fail to protect personal data?**
    - Organizations that fail to protect personal data under RA 10173 may face heavy fines, jail time, and lawsuits. This is to ensure that personal information is always kept safe and private.

Violation	Possible Fine	Imprisonment	Example
Unauthorized processing of personal data	₱500,000 – ₱2,000,000	1-3 years	A company uses your data without your consent.
Access due to negligence	₱500,000 – ₱4,000,000	1.5-3 years	An organization fails to secure its database, leading to leaks.
Improper disposal of personal data	₱500,000 – ₱2,000,000	1-3 years	Throwing documents with personal info in the trash without shredding.
Unauthorized disclosure	₱500,000 – ₱5,000,000	1.5-5 years	An employee shares customer data with outsiders.
Malicious disclosure	₱500,000 – ₱5,000,000	3-5 years	Selling or purposely leaking private records.
Unauthorized access (intentional)	₱500,000 – ₱2,000,000	1-3 years	Hacking into a system to steal personal data.

5. **In what cases can an individual demand erasure of their personal data?**
    - Under the Data Privacy Act of 2012 (RA 10173), a person can ask for their data to be erased if it is no longer needed, wrong, outdated, or collected without permission. They can also demand erasure if they take back their consent or if the data is being used in the wrong way. This right protects people from misuse of their personal information.

Application Scenarios:

- **Scenario 1:** Online Shopping Platform Breach A popular online shopping platform experienced a security breach, resulting in the exposure of thousands of customers' personal information, including their names, addresses, and credit card details.

Questions:

How should the company respond to this data breach under RA 10173?

- The company must report the breach to the National Privacy Commission (NPC) and inform affected customers right away. It should secure its system, investigate the cause, and provide remedies like account protection or credit monitoring. The company must also strengthen its security measures to prevent future breaches.

What rights do the affected customers have in this situation?

- Customers have the right to be informed about the breach and the right to access their exposed data. They may request rectification if information is wrong, demand erasure or blocking if they feel unsafe, and even claim damages if they suffer harm. These rights ensure their personal information is protected even after a breach.

- **Scenario 2:** School Enrollment Database A school collects sensitive personal information such as health records, family backgrounds, and grades during the enrollment process.

Questions:

What steps must the school take to ensure compliance with RA 10173?

- The school must collect only necessary data with consent and keep it safe in secure systems. Access should be limited to authorized staff, and clear privacy policies must be in place. If a data breach happens, the school must report it to the National Privacy Commission (NPC).

If a former student requests that their personal information be erased from the school's records, how should the school handle this request?

- The school must carefully review the request and balance it with legal obligations. Some records, such as grades and transcripts, are considered permanent academic records and cannot be fully erased because they are needed for verification in the future. However, other personal data that is no longer necessary, like health declarations or contact details, may be deleted or anonymized.

- **Scenario 3:** Job Application Process A company collects resumes and application forms from candidates. One candidate later learns their personal information was shared with another company without their consent.

Questions:

Has the company violated RA 10173? If so, what are the consequences?

- Yes, the company violated RA 10173 because it shared the candidate's personal information with another company without consent. This is considered unauthorized disclosure of personal information, which is punishable by fines ranging from ₱500,000 to ₱5,000,000 and imprisonment of 1.5 to 5 years for those responsible. The candidate may also claim damages if the disclosure caused harm, such as identity theft or discrimination.

What should the company have done differently to comply with the law?

- The company should have obtained clear and informed consent from the candidate before sharing any personal data with another organization. It must also limit the use of the candidate's information strictly for recruitment purposes and ensure that privacy policies are explained during the application process. By doing this, the company would respect the candidate's rights and remain compliant with RA 10173.

Part B. RA 10175 – Cybercrime Prevention Act of 2012

1. **What are the three categories of cybercrime offenses under RA 10175?**

Category	Meaning	Examples
1. Offenses against the confidentiality, integrity, and availability of computer data and systems	Crimes that attack computer systems or data directly.	Hacking (illegal access), spreading viruses, deleting or altering files, blocking websites.
2. Computer-related offenses	Crimes done using computers to commit fraud or deception.	Online identity theft, credit card fraud, computer forgery.
3. Content-related offenses	Crimes involving illegal or harmful online cntent.	Cybersex, child pornography, online libel (false/damaging posts).

2. **How is online libel different from traditional libel?**
    - Traditional libel happens when someone writes or publishes false and damaging statements against another person in printed or physical forms like newspapers, magazines, or flyers. On the other hand, Online libel, under RA 10175 (Cybercrime Prevention Act of 2012), happens when the same false and damaging statements are posted or shared through digital means such as social media, blogs, forums, or websites. The main difference is that traditional libel is in print or physical media, while online libel is through the internet or electronic platforms, which can reach a wider audience faster.
3. **Why does RA 10175 impose heavier penalties for crimes against critical infrastructures?**
    - RA 10175 (Cybercrime Prevention Act of 2012) imposes heavier penalties for crimes against critical infrastructures because these systems are essential to public safety, national security, and the economy. Critical infrastructures include government networks, banking systems, hospitals, transportation, energy, and communication services. If these systems are attacked or disrupted, the effects can be very serious like shutting down hospitals, disrupting power grids, exposing government secrets, or collapsing financial transactions. Since the damage could affect millions of people, the law gives stricter punishments to discourage attackers and protect the country from large-scale harm.
4. **Can a Filipino abroad be prosecuted under RA 10175? Why or why not?**
    - Yes, a Filipino abroad can still be prosecuted under RA 10175 (Cybercrime Prevention Act of 2012) because the law has extraterritorial application. This means it can apply even if the crime is committed outside the Philippines, as long as the act is committed by a Filipino citizen or resident, or the crime targets a Filipino, a Philippine-based system, or has effects in the Philippines.
5. **How does RA 10175 empower law enforcement in investigating cybercrimes?**
    - RA 10175 empowers law enforcement by giving them special authority and tools to investigate cybercrimes. They can collect and preserve electronic evidence, track and block illegal online activities, and order service providers to disclose relevant computer data. The law also allows them to seize or restrict access to

computer systems used for crimes, conduct real-time traffic monitoring, and coordinate with international agencies when crimes cross borders.

Application Scenarios:

- **Scenario 1:** Hacking a Business Website A hacker gains unauthorized access to a local business's website, altering its content and stealing customer data.

Questions:

What provisions of RA 10175 has the hacker violated?

- The hacker has violated provisions against illegal access (unauthorized entry into a computer system), data interference (stealing or altering customer data), and system interference (changing the website's content). If the stolen data includes personal or financial details, it may also fall under computer-related fraud and identity theft.

What actions can the business take under the law to protect itself and its customers?

- The business should immediately report the incident to law enforcement and the National Bureau of Investigation (NBI) Cybercrime Division. It must also notify affected customers, secure its systems to stop further breaches, and preserve digital evidence for investigation. Under RA 10175, the business can request authorities to track, block, or restrict access to the hacker's activities, while also strengthening its cybersecurity measures to prevent future attacks.

- **Scenario 2:** Cyberbullying Incident A student posts defamatory and malicious statements about a classmate on social media, leading to harassment and emotional distress.

Questions:

How does RA 10175 address online libel and cyberbullying?

- RA 10175 punishes online libel, which includes defamatory posts made on social media. Cyberbullying, while not directly named, is covered when the posts cause harassment or emotional harm. The law imposes stricter penalties than traditional libel because online posts spread faster.

What legal actions can the victim take, and what penalties could the perpetrator face?

- The victim can file a complaint with the NBI Cybercrime Division or PNP Anti-Cybercrime Group and seek damages in court. The perpetrator may face 6 months to 6 years in prison and fines of ₱200,000 to ₱1,000,000.

- **Scenario 3:** Online Scam An individual creates a fake online store, tricking customers into paying for products that do not exist.

Questions:

Which computer-related offenses under RA 10175 has the scammer committed?

- The scammer committed computer-related fraud by tricking customers into paying for fake products, and possibly identity theft if another person's details were used.

How can law enforcement trace and prosecute the scammer, and what penalties could they face?

- Authorities can track the scammer using IP addresses, payment records, and digital footprints. If found guilty, the scammer may face 6–12 years of imprisonment and fines up to ₱1,000,000.

- **Scenario 4:** Cybersex Operation A group is discovered running an illegal cybersex operation using video streaming services, involving the exploitation of minors.

Questions:

How does RA 10175 address cybersex, particularly when it involves minors?

- RA 10175 directly prohibits cybersex operations, especially when they exploit minors. This act is considered a serious crime because it violates human dignity, children's rights, and public morals. The law classifies cybersex involving minors as a grave offense, subject to heavy punishment.

What legal steps should authorities take to stop the operation, and what penalties will the offenders face?

- Authorities must rescue the victims, close the illegal platforms, and gather digital evidence. Offenders face up to 12 years in prison and fines up to ₱1,000,000, plus additional penalties under child protection laws.

Part C. Reflection - Why These Laws Matter?

1. **Why are RA 10173 and RA 10175 important in today's digital society?**
    - In today's digital world, RA 10173 (Data Privacy Act) and RA 10175 (Cybercrime Prevention Act) are very important because they help keep people safe online. Many of us use social media, online shopping, and digital payments, and these laws protect us from risks like hacking, scams, and misuse of personal information.
2. **How do these laws protect both individuals and organizations?**
    - These laws protect individuals by making sure their personal data is safe and giving them rights like checking or asking to erase their data. They also protect organizations by giving rules on how to handle information properly, which builds trust with customers and avoids problems like data breaches.
3. **As future IT professionals, what role will you play in upholding these laws?**
    - As future IT professionals, we need to follow and respect these laws. Our role is to create secure systems, protect people's data, and make sure technology is used in the right way. By doing this, we help make the online world safer and more trustworthy for everyone.

References

Lawphil. (2012). Republic Act No. 10175: Cybercrime Prevention Act of 2012. https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html

National Privacy Commission. (2012). Republic Act No. 10173: Data Privacy Act of 2012. https://privacy.gov.ph/data-privacy-act/

Respicio, H. (2024, November 8). *Rights of data subject | R.A. No.10173 or the Data Privacy Act | OTHER SPECIAL LAWS AND RULES*. RESPICIO & CO. https://www.respicio.ph/bar/2025/mercantile-and-taxation-laws/other-special-laws-and-rules/ra-no10173-or-the-data-privacy-act/rights-of-data-subject

Respicio, H. (2025, June 24). *Cyber libel in the Philippines: elements and penalties*. RESPICIO & CO. https://www.respicio.ph/commentaries/cyber-libel-in-the-philippines-elements-and-penalties

Oatemar, A. P. (2025, January 13). *Fast Facts: Data Privacy Act (RA 10173)*. https://sprout.ph/articles/data-privacy-act-101/

SC: For online libel, courts may impose alternative penalty of fine instead of imprisonment – Supreme Court of the Philippines. (n.d.). https://sc.judiciary.gov.ph/sc-for-online-libel-courts-may-impose-alternative-penalty-of-fine-instead-of-imprisonment/

University of Minnesota Human Rights Library. (n.d.). https://hrlibrary.umn.edu/research/Philippines/RA_10175.html