Part A. RA 10173 - Data Privacy Act of 2012

Study Questions:

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

   Personal information refers to basic details that can identify someone, such as name, address, or phone number. Sensitive personal information is more private and needs extra protection because it can harm or discriminate against a person if misused. Examples include health records, financial details, or religion. Privileged information is data shared in a special professional relationship that must remain confidential, like a lawyer-client conversation or doctor-patient notes.

2. **What is the role of the DPO in ensuring compliance with RA 10173?**

   The Data Protection Officer (DPO) makes sure that an organization follows the Data Privacy Act. The DPO trains staff about data privacy, checks that personal data is handled properly, and responds to complaints or questions about privacy. They also act as the bridge between the organization and the National Privacy Commission.

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

   One right is the right to access, which means people can ask organizations what personal data they have about them. For example, a customer can ask a bank for a copy of their records. Another right is the right to correct, which allows people to fix wrong or outdated information. For example, if a school has the wrong birthdate of a student, the student can ask them to correct it.

4. **What penalties await organizations that fail to protect personal data?**

   Organizations that fail to protect personal data can face heavy fines and even imprisonment of responsible officers. They may also lose the trust of their customers and face lawsuits. For example, if a company leaks credit card details of its clients, it can be penalized and ordered to pay damages to those affected.

5. **In what cases can an individual demand erasure of their personal data?**

   An individual can demand erasure of their data when the information is no longer needed for its purpose, when they withdraw their consent, or when the data is being used unlawfully. For example, if a person unsubscribes from a service, they can ask the company to delete their contact details.

Application Scenario:

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:

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

   Under RA 10173, the company must immediately act after the breach by reporting it to the National Privacy Commission (NPC) within 72 hours and informing all affected customers that their names, addresses, and credit card details were exposed. It must investigate and contain the breach to prevent further harm, identify the weaknesses that caused it, and apply stronger security measures such as encryption and stricter access controls.

2. **What rights do the affected customers have in this situation?**

   The affected customers have several rights under RA 10173. They have the right to be informed about what happened and how their personal data was compromised. They also have the right to access their personal data that the company still stores, the right to request corrections if any of their data is inaccurate, and the right to erase or block if the data is no longer necessary.

Scenario 2: School Enrollment Database

A school collects sensitive personal information such as health records, family backgrounds, and grades during the enrollment process.

Questions:

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

   The school must make sure it only collects information that is truly necessary for enrollment and academic purposes. Before collecting any data, it should obtain clear consent from parents and students, explaining why the data is needed and how it will be used. The school must also ensure that the data is stored securely. Only authorized school personnel should have access to the information, and all staff must be educated about data privacy responsibilities.

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

   If a former student requests erasure of their personal data, the school must carefully review the request. If the data is no longer needed for academic or legal purposes, the school should delete it securely. However, if the information must be retained due to legal or government requirements, such as records of grades, transcripts, or graduation verification, then the school is not allowed to delete it.

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:

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

   Yes, the company has violated RA 10173 because it shared an applicant's personal information with another company without the applicant's consent. This is considered unauthorized processing and disclosure of personal data, which is prohibited by the law. The violation can lead to administrative fines, civil liabilities such as payment of damages to the affected individual, and even criminal penalties where responsible officers may face imprisonment.
2. **What should the company have done differently to comply with the law?**

   The company should have asked for the applicant's consent before sharing any personal information with another company. It should have used the resumes and application forms strictly for the hiring process only, and not for any other purpose outside of the applicant's knowledge.

PART B. RA 10175 - Cybercrime Prevention Act of 2012
Study Questions:

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

   RA 10175 divides cybercrimes into three main categories. The first is offenses against confidentiality, integrity, and availability of data and systems, which include illegal access, hacking, data interference, and system interference. The second category is computer-related offenses such as computer forgery, fraud, and identity theft. The third category covers content-related offenses like cybersex, child pornography, and online libel. These three categories cover most of the serious crimes that happen in the online world.
2. **How is online libel different from traditional libel?**

   Traditional libel usually happens in print, newspapers, or public speeches, while online libel happens over the internet through social media, blogs, websites, or emails. Online libel can spread faster and reach more people instantly compared to traditional libel, which is why the law considers it more damaging. The digital nature of online libel makes it more difficult to control, which justifies the heavier penalties under RA 10175.
3. **Why does RA 10175 impose heavier penalties for crimes against critical infrastructures?**

   RA 10175 imposes heavier penalties for attacks on critical infrastructures because these systems are essential to national security, public safety, and economic stability. Examples include government databases, hospitals, banks, airports, energy grids, and

communication networks. If these are attacked or disrupted, millions of people could be affected at once, leading to chaos or danger to lives.

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 because the law has extraterritorial application. This means that if a cybercrime is committed by a Filipino outside the Philippines, or if the crime affects a Filipino or Philippine systems even if the offender is abroad, the law still applies. This ensures that Filipinos remain accountable for their actions online no matter where they are in the world.

5. **How does RA 10175 empower law enforcement in investigating cybercrimes?**

   RA 10175 gives law enforcement agencies special powers to investigate cybercrimes. They are allowed to collect and record real-time traffic data such as IP addresses and online activity. They can also order internet service providers and other companies to preserve and disclose computer data needed for investigations. With proper court orders, law enforcement can search and seize digital evidence from devices or servers.

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:

1. **What provisions of RA 10175 has the hacker violated?**

   The hacker in this situation has violated several provisions of RA 10175, such as illegal access, data interference, and misuse of computer data. The business can file a case against the hacker under RA 10175 and seek legal remedies.

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

   Report the crime to authorities immediately to protect its customers. At the same time, the business must upgrade its cybersecurity measures to prevent future attacks and reassure its customers that their data will be safe moving forward.

Scenario 2: Cyberbullying Incident

A student posts defamatory and malicious statements about a classmate on social media, leading to harassment and emotional distress.

Questions:

1. **How does RA 10175 address online libel and cyberbullying?**

   RA 10175 addresses this problem through online libel and other harmful online acts. In this case, the victim of cyberbullying has the right to file a complaint with authorities and present proof such as screenshots of the malicious posts.

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

   The perpetrator may face imprisonment and fines depending on the severity of the crime. If the victim is a minor, the law provides even stricter protection, and the penalties against the bully will be heavier. This ensures that online harassment is taken seriously under the law.

Scenario 3: Online Scam

An individual creates a fake online store, tricking customers into paying for products that do not exist.

Questions:

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

   In this case, the scammer has committed computer-related fraud and identity theft, both of which are punishable under RA 10175. Law enforcement can trace the scammer by tracking IP addresses, payment channels, and online activities, often with the help of internet service providers and banks.
2. **How can law enforcement trace and prosecute the scammer, and what penalties could they face?**

   The scammer may face imprisonment of up to 12 years, along with heavy fines depending on the money stolen. The law provides a clear process for catching and prosecuting scammers to protect consumers.

Scenario 4: Cybersex Operation

A group is discovered running an illegal cybersex operation using video streaming services, involving the exploitation of minors.

Questions:

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

   RA 10175 clearly states that cybersex operations are illegal, especially when they involve minors. This activity is considered a form of exploitation and is heavily punished by the law. In this scenario, authorities must immediately shut down the operation, rescue and protect the minors, arrest the offenders, and preserve the digital evidence such as video files.
2. **What legal steps should authorities take to stop the operation, and what penalties will the offenders face?**

   The penalties include long-term imprisonment and high fines, with even harsher penalties if minors are involved. This shows how the law prioritizes protecting vulnerable individuals from online exploitation.

PART C. Reflection

Write a short essay / reflection answering:

1. **Why are RA 10173 and RA 10175 important in today's digital society?**

   RA 10173 and RA 10175 are very important in today's digital society because they protect people from risks that come with using technology. With the growth of online shopping, online banking, social media, and digital learning, personal information and online activities are constantly at risk of being misused. RA 10173 protects individuals by ensuring that their personal information is handled properly and securely, while RA 10175 punishes those who use technology to commit crimes such as hacking, scams, online libel, and cybersex.

2. **How do these laws protect both individuals and organizations?**

   These laws provide protection not only to individuals but also to organizations. For individuals, they protect against identity theft, online harassment, scams, and misuse of private information. For organizations, these laws provide guidelines on how to handle data properly and offer legal remedies if they are victims of cybercrimes. By ensuring both sides are protected, the laws create a safer and more trustworthy digital environment.

3. **As future IT professionals, what role will you play in upholding these laws?**

   As future IT professionals, we have a big role in upholding these laws. Our responsibility is to design and maintain systems that respect privacy and are safe from attacks. We must also promote ethical use of technology and educate others on safe online practices. By following RA 10173 and RA 10175, we help ensure that technology remains a tool for progress and not for harm. These laws remind us that while technology brings many benefits, it must always be guided by responsibility and respect for others.