--Question Starting--

1. Consider the following scenarios related to Sections 66C, 66D, 67, and 67A of the IT Act 2000/2008:

I. A person creates a fake email account using another individual's personal information and uses it to solicit funds from the public.

II. An individual digitally alters explicit images of a person without consent and disseminates them on social media platforms.

III. Using a fraudulent digital identity, someone impersonates a government official to secure sensitive information from citizens.

IV. A company inadvertently leaks user data due to insufficient security measures, leading to unauthorized access to personal information.

V. An individual sends emails containing obscene content using their own legally registered email address.

Choose the correct answer from the options given below:

(1) I, II, and III only

(2) II, III, and IV only

(3) I, III, IV, and V only

(4) I, II, and III only

Answer Key: 4

Solution:

? Statement I(Correct): This scenario directly relates to Section 66D, which deals with cheating by personation using computer resources. Creating a fake email for soliciting funds fits this violation.

? Statement II(Correct): This falls under Section 67A, which penalizes the electronic publication or transmission of material containing sexually explicit acts or conduct in electronic form without consent.

? Statement III(Correct): Again, this pertains to Section 66D of the IT Act, which covers the offense of personation using electronic means, particularly when done to deceive or harm others.

? Statement IV(Incorrect): This situation might involve a breach of reasonable security practices under Section 43A of the IT Act, which is not listed among the sections we are focusing on (66C, 66D, 67, 67A).

? Statement V(Incorrect): While distasteful, sending obscene content using one's own email does not fall under the specified sections if not involving deceit or explicit material as defined under Section 67 or 67A.

Hence, Option (4) is the right answer.

--Question Starting--

2. Consider these practices in the context of data anonymization, pseudonymization, and de-identification:

I. Removal of all direct identifiers from a dataset, ensuring no specific individual can be identified.

II. Process of replacing personal identifiers in a dataset with artificial identifiers or pseudonyms.

III. Data manipulation where original data values are replaced with values that preserve statistical distributions but are unrelated to the true values.

IV. A method where data is encrypted using a key, which the processor retains, allowing for potential re-identification.

V. Application of a statistical method to blur data, such as adding random noise to each data point in a set.

Choose the correct answer from the options given below:

(1) I, III, and V only

(2) II, IV, and V only

(3) I, II, and IV only

(4) I, II, and V only

Answer Key: 1

Solution:

? Statement I(Correct): This describes a de-identification technique where direct identifiers are removed to prevent the identification of individuals, adhering to privacy laws and guidelines.

? Statement III(Correct): This refers to data masking or synthetic data generation, a form of anonymization where true values are replaced but statistical integrity is maintained.

? Statement V(Correct): Adding random noise is a method of differential privacy, a technique used in anonymization to enhance privacy while preserving the utility of the data.

? Statement II(Incorrect): Replacing identifiers with pseudonyms defines pseudonymization, not

anonymization; the data can still potentially be re-identified if additional information becomes available.
? Statement IV(Incorrect): Encryption with retained keys is a form of pseudonymization; the data remains reversible and does not achieve full anonymization.
Hence, Option (1) is the right answer.

--Question Starting--
3. Analyze the implications of Foucault?s concept of the Panopticon and disciplinary power in the following contexts:
I. A corporation uses extensive surveillance to monitor employee productivity and enforce corporate policies.
II. A government employs city-wide CCTV surveillance to deter criminal activities and enforce law.
III. An online platform uses algorithms to monitor user behavior and personalize content delivery.
IV. A teacher uses a point system where students' behavior is constantly monitored and rewarded.
V. A social media company analyzes user data to predict and influence purchasing behaviors.
Choose the correct answer from the options given below:
(1) I, II, and IV only
(2) I, III, IV, and V only
(3) II, III, and IV only
(4) II, IV, and V only
Answer Key: 1
Solution:
? Statement I(Correct): This scenario closely aligns with Foucault's Panopticon, where surveillance is used as a tool of power and control within a disciplinary institution, in this case, a corporation.
? Statement II(Correct): The use of CCTV by governments as a means of societal control and deterrence through constant surveillance also reflects the principles of the Panopticon.
? Statement IV(Correct): The educational use of a point system for behavior monitoring and rewards mimics the Panopticon?s concept of continuous observation linked to disciplinary power, shaping and controlling behavior.
? Statement III(Incorrect): While online platforms monitor user behavior, the primary intent here is content personalization rather than disciplinary power or social control, thus slightly diverging from Foucault?s original concept of the Panopticon.
? Statement V(Incorrect): Analyzing user data for predicting purchasing behaviors involves manipulation and economic exploitation more than disciplinary power in its traditional Foucauldian sense.
Hence, Option (1) is the right answer.