Centre for Aerospace & Defence Laws (CADL)
DIRECTORATE OF DISTANCE EDUCATION
NALSAR UNIVERSITY OF LAW, HYDERABAD

M.A. (Security & Defence Laws)

Academic Year: 2023-2024
Third Semester Repeat Examination (June, 2024)

Paper IV – 2.3.12. Cyber Space, Cyber Security and National Defence

Duration of the Examination: 2 ½ hours **Total Marks: 70 marks**

INSTRUCTIONS TO CANDIDATES

a) **Read the instructions carefully and adhere to the same.**
b) **Please mention your DDE ID No., date of the exam, name of the programme & subject on the Answer Sheet and the Additional Answer Sheets, if any.**
c) **The questions to be interpreted as given and no clarification can be sought from the Invigilator.**
d) **Clearly indicate the question numbers while answering them. Answers without question numbers / wrong question numbers will not be evaluated.**
e) **Write the answers clearly and neatly. Answers in illegible handwriting will not be taken into consideration.**
f) **Candidates are prohibited to carry phones or any other electronic devices, books, material etc. in the Examination Hall.**
g) **Copying is strictly prohibited and is considered as a serious academic mis-conduct and the University will take action as it deems fit.**

Section – A

Answer FIVE questions out of SEVEN questions and each question carries 10 marks. (5 x 10 marks = 50 marks)

1. Discuss the effectiveness of the Information Technology Act, 2000 (IT Act) in addressing cybersecurity challenges in India, focusing on Section 43A and Section 66F. What are the strengths and limitations of these sections in combating cybercrimes, and what improvements are needed to enhance cyber security measures?

2. Analyse how the concepts of 'actus reus' (the physical act of the crime) and 'mens rea' (the intent to commit the crime) are applied in prosecuting cyber crimes under the Information Technology Act, 2000. Consider a scenario where an individual unintentionally releases a malware that causes significant damage. How might the court determine the presence or absence of 'mens rea' and 'actus reus' in this case, and what could be the legal consequences for the individual involved?

3. Given the recent surge in cyber pornography cases, such as the arrest linked to the circulation of illicit content through encrypted platforms, critically analyze the provisions under the IT Act, particularly Section 67, which deals with the publication or transmission of obscene material in electronic form. How effective are these provisions in curbing the spread of cyber pornography? What additional measures could be implemented to strengthen these laws?

4. Reflect on the significant data breach at a major Indian e-commerce company where personal data of millions of users was compromised. Discuss the applicability of Section 43A of the IT Act, which pertains to compensation for failure to protect data. Evaluate whether the current legal framework adequately incentivizes companies to invest in robust cybersecurity measures. What revisions could be made to this section to enhance data protection?

5. In light of recent controversies involving social media platforms and their management of user-generated content, analyze the responsibilities and liabilities of intermediaries under Section 79 of the IT Act. How does this section balance between curtailing harmful online content and protecting the freedom of expression? Considering global trends and incidents, should there be stricter regulations imposed on intermediaries to ensure compliance with cybersecurity norms?

6. Reflect on the 2021 incident where data from an Indian airline's servers, located overseas, were leaked. Discuss how the IT Act deals with cross-border data issues and the challenges involved in enforcing legal actions against foreign entities. What mechanisms are currently in place under the IT Act to handle such scenarios, and what improvements are required to address the jurisdictional challenges in cybercrimes?

7. In August 2023, "ShopTrendy," an Indian online retail company, experienced a significant data breach. An unauthorized access to their database resulted in the leakage of personal data, including names, addresses, credit card details, and purchase history of approximately 3 million customers. Preliminary investigations suggest that the breach was due to insufficient security measures, such as outdated encryption methods and lack of regular security audits. Customers affected by the breach have reported unauthorized transactions and privacy violations, sparking widespread criticism and calls for legal action.

As a cybersecurity legal consultant, you have been approached to provide a detailed analysis of the situation concerning the Information Technology Act, 2000. Based on Section 43A and any relevant provisions on:

I. Evaluate the legal liabilities of "ShopTrendy" for the data breach.
II. Discuss the possible legal actions that the affected customers can initiate against "ShopTrendy."
III. Recommend preventive measures that "ShopTrendy" should implement immediately to comply with the IT Act and to prevent future breaches.

Section – B

Answer FOUR questions out of SIX questions and each question carries 05 marks. (4 x 5 marks = 20 marks)

A. Discuss the role of the Indian Computer Emergency Response Team (CERT-In) as defined under the IT Act.

B. How does the IT Act address data privacy issues?

C. How does Section 79 provide a safe harbor for intermediaries, and what are the conditions attached to this exemption?

D. How does the IT Act categorize different cyber offenses, and what are the typical legal consequences for such crimes?

E. Explain how the IT Act governs the use of digital signatures and electronic records.

F. Discuss recent amendments to the IT Act to address the evolving nature of cyber threats and technology?