SHORT QUESTIONS BANK

1. What is a cyberspace?
2. List the key objectives of cyber laws.
3. Recall any three types of cybercrimes prevalent in India.
4. Define the term ‘cyber ethics’.
5. Identify any two challenges faced in enforcing cyber law.
6. What is the importance of cyber laws in today’s digital society?
7. Explain the concept of Right to Privacy in cyberspace.
8. Define the meaning of phishing with an example.
9. What is cyber defamation?
10. State any two penalties under the IT Act, 2000.
11. Define cyber terrorism.
12. Illustrate the meaning of cyber stalking.
13. Define the term ‘electronic record’ under the IT Act.
14. What is an electronic signature certificate?
15. Explain the duties of a subscriber under the IT Act.
16. What are the objectives of the Information Technology Act, 2000?
17. List three major functions of the Cyber Appellate Tribunal.
18. Explain the concept of ‘identity theft’ in cyberspace.
19. Identify the meaning of ‘cyber pornography’.
20. What is the role of a Certifying Authority under the IT Act?
21. Explain the meaning of ‘ISP’ and their legal obligations.
22. What are jurisdictional issues in cyberspace?
23. Define the term “Right to access cyberspace.”
24. What are e-commerce disputes and how are they regulated?
25. Utilize the significance of digital signatures in online transactions.
26. Explain the role of the government in regulating e-commerce.
27. What is the significance of ethics in AI and Machine Learning applications?
28. Identify the duties of the Controller of Certifying Authorities (CCA).
29. What is the role of dispute resolution mechanisms in cyber law?
30. Demonstrate the duties of intermediaries under Section 79 of the IT Act.
31. What are the essential features of the Digital Personal Data Protection Act, 2023?
32. Explain the concept of cyber peace and its importance.
33. Compare the difference between hacking and ethical hacking.
34. What are the duties of users in maintaining cyber hygiene?
35. What is the relationship between cyber law and human rights?
36. Analyze the effectiveness of the IT Act, 2000 in combating cybercrime.
37. Analyze the role of ethical practices in reducing cyber crimes.
38. Evaluate how cyber law addresses the challenges of freedom of expression.
39. Evaluate the need for cyber ethics in professional environments.
40. Analyze how cyber crimes impact e-commerce businesses.
41. Evaluate the importance of jurisdiction in handling cybercrime.
42. Analyze the challenges of implementing Online Dispute Resolution (ODR).

43. Evaluate the relevance of the Digital Personal Data Protection Act, 2023 in today's context.
44. Analyze the implications of cyber defamation on individual rights.
45. Evaluate how intermediaries can prevent the spread of fake news.
46. Analyze the risks of not practicing cyber hygiene for students.
47. Evaluate the role of digital literacy in preventing cybercrime.
48. Analyze the impact of cyber terrorism on national security.
49. Evaluate the ethical concerns surrounding surveillance in cyberspace.
50. Analyze the role of international cooperation in combating cybercrime.
51. Define cyberspace and explain its key features.
52. Illustrate the impact of computers on modern society.
53. List and describe any three types of cybercrimes against individuals.
54. Explain the legal significance of the Right to Privacy in cyberspace.
55. Evaluate the effectiveness of civil remedies under the IT Act, 2000.
56. List any three advantages of using computers in law enforcement.
57. Explain the concept of Cyber Harassment with an example.
58. Identify and describe three civil wrongs under the IT Act, 2000.
59. Illustrate the significance of freedom of speech in cyberspace.
60. Apply the IT Act provisions to a case of cyber defamation.
61. Define phishing and explain how it affects users.
62. Summarize the objectives of the Information Technology Act, 2000.
63. Describe the term "Cyber Terrorism" and its legal implications.
64. Demonstrate the role of jurisdiction in cyber disputes.
65. Evaluate the effectiveness of dispute resolution mechanisms in cyber law.
66. What is identity theft and how is it committed online?
67. Explain the term "Right to Access Cyberspace."
68. Apply the IT Act provisions to a case of hacking into a corporate system.
69. List and explain three regulatory roles played by the government in e-commerce.
70. Explain the role of digital evidence in cybercrime investigations.
71. Evaluate whether the IT Act adequately covers cyber pornography.
72. Define cyber defamation and its legal consequences.
73. Illustrate the types of cybercrime against institutions.
74. Apply constitutional protections to online hate speech.
75. Analyze the challenges in enforcing jurisdiction in international cybercrime cases.
76. Define cyber stalking and mention its legal remedy.
77. Explain the objectives of Cyber Law in India.
78. Apply the law to a situation where someone circulates morphed images of another person.
79. List three emerging threats in cyberspace.
80. Interpret the concept of e-Governance under the IT Act.
81. Evaluate the role of the judiciary in protecting digital privacy in India.
82. Define hacking and identify applicable legal provisions.
83. Demonstrate the legal framework for data protection under Indian cyber law.
84. Apply the concept of intermediary liability in social media regulation.

85. Analyze the limitations of the IT Act, 2000 in today's digital ecosystem.
86. Analyze the impact of cybercrime on individual privacy.
87. Evaluate the effectiveness of the IT Act in combating cyber terrorism.
88. Analyze the role of the judiciary in regulating freedom of expression online.
89. Evaluate the need for international cooperation in cybercrime regulation.
90. Analyze how social media fuels cyber defamation.
91. Evaluate the effectiveness of current cyber forensics practices in India.
92. Analyze the challenges of digital consent under the DPDP Act, 2023.
93. Evaluate India's preparedness against AI-enabled cybercrimes.
94. Analyze how e-governance platforms are vulnerable to cyber attacks.
95. Evaluate the role of grievance redressal mechanisms in ensuring digital justice.
96. Analyze the conflict between surveillance and privacy in the digital age.
97. Evaluate the impact of misinformation on public order through cyberspace.
98. Analyze the challenges of enforcing cyber law in rural India.
99. Evaluate whether existing laws adequately protect women in cyberspace.
100. Analyze the role of ethical hacking in national cybersecurity.
101. Evaluate the effectiveness of Section 43A in ensuring corporate data protection.
102. Analyze the pros and cons of internet shutdowns as a tool for law enforcement.
103. Evaluate the contribution of CERT-IN in combating cyber threats in India.
104. Analyze the implications of storing data on foreign servers for Indian users.
105. Evaluate the limitations of traditional laws in addressing modern cyber offenses.