NEW SYLLABUS

544

Roll No. .....

OPEN BOOK EXAMINATION

Time allowed : 3 hours

Maximum marks : 100

Total number of questions : 4

Total number of printed pages : 15

NOTE : *Answer* ***ALL*** *Questions.*

1. In a high-level management discussion at Zedtronics Solutions Ltd, a leading technology firm, the legal team, Artificial Intelligence (AI) researchers, and Compliance personnel gathered to explore the evolving complexities of artificial intelligence, copyright laws, and digital regulations. The discussion was triggered by a real-time scenario–an AI-powered content generator recently developed by the Company that could produce unique works of music, text and design. This innovation had already been used in various projects, leading to an internal debate about the ownership and copyrightability of AI-generated content.

The legal team pointed out that the current copyright framework primarily recognizes human authorship. Some experts argued that since AI models are trained using vast datasets, the developers who curate these datasets and fine-tune the model should hold the copyright. Others emphasized that users who direct the AI's output through specific instructions play a crucial creative role and should, therefore, be granted authorship. One of the AI researchers noted that AI-generated works often combine existing ideas in novel ways without direct human input, raising concerns about whether such works meet the originality threshold required for copyright protection. Some jurisdictions had recently acknowledged AI-generated works

by assigning authorship to the person initiating the creative process, whereas others remained firm that only humans could hold intellectual property rights. Additionally, the risk of monopolistic control over AI-generated content was highlighted, as granting rights to developers could lead to restrictive licensing models, limiting creativity and access for end users.

The conversation then transitioned to the broader regulatory landscape, particularly the government's evolving approach to digital governance. With increasing dependence on digital platforms, a newly introduced regulation aimed at structuring compliance in the online space had sparked debate. The compliance officer explained that small and medium-sized enterprises (SMEs) were particularly vulnerable, as they often lacked the resources to implement extensive compliance measures. Content creators and online businesses also faced challenges concerning new standards for digital platforms. While ensuring accountability was essential, overly rigid measures could risk stifling creativity and engagement, potentially leading to excessive content takedowns. The discussion also touched on the issue of data localization, with questions raised about the implications for global trade and the ability of businesses to store information across borders. Some felt that enforcing data localization could strengthen national security, while others warned of the economic and operational challenges for companies navigating multi-jurisdictional regulations.

Another pressing concern in the discussion was the increased reliance on digital records in legal proceedings. The legal department referenced recent case where manipulated digital evidence had led to an erroneous judicial outcome, underscoring the risks associated with electronic

documentation. Company's compliance experts stressed the importance of implementing stringent verification mechanisms, including emerging technologies such as blockchain for secure documentation. However, challenges remained in distinguishing between accidental errors and deliberate falsification, raising the question of how accountability should be structured in such cases. There was also a discussion on whether the legal system was adequately equipped to assess digital evidence and whether new forensic methodologies needed to be standardized across courts.

As the meeting progressed, the focus shifted to evolving challenges in data security, privacy concerns, and customer relationship management, the leadership team recognized the need for a strategic approach to technology integration that aligns with business objectives.

The conversation concluded with reflections on the broader impact of these legal and regulatory developments. While technological advancements offered immense opportunities for innovation, there was a growing need for balanced legal frameworks that protected stakeholders without hindering progress. As AI and digital regulations continued to evolve, organizations had to remain agile, adapting their compliance strategies to align with emerging legal standards.

In the light of above case scenario, answer the following questions :

(*a*) You being in the legal team of Zedtronics Solutions suggest, should the law evolve to recognize AI-generated content, and if so, who should be the rightful copyright holder ? Support your answer with a case law.

(*5 marks*)

(*b*) In the light of a judicial precedent of a case in the Delhi High Court, regarding the issue of whether an AI generated work can be copyrighted in India, comment whether granting copyright to AI developers encourages innovation or creates monopolistic control ?

(*5 marks*)

(*c*) What are the key concerns which Zedtronics Solutions Ltd may face in balancing business interests, individual privacy, and national security under new digital regulations i.e., Digital India Act 2023 ?

(*5 marks*)

(*d*) *"Company's compliance experts stressed the importance of implementing stringent verification mechanisms, for secure documentation. However challenges remained in distinguishing between accidental errors and deliberate falsification, raising the question of how accountability should be structured in such cases."* In the light of the above statement state how can legal frameworks effectively differentiate between unintentional mistakes in digital records and the deliberate fabrication of electronic evidence in judicial proceedings ?

(*5 marks*)

(*e*) Explain the significance of data privacy as a fundamental right and outline the key challenges individuals face in protecting their personal information online.

(*5 marks*)

2. The risk management committee and the senior leadership team of a Paythen Ltd, a major fintech company and Kyuthen Ltd, its e-commerce subsidiary convened for a strategic cybersecurity review. As both companies expanded their digital presence, concerns over cybersecurity threats, regulatory compliance, and operational risks became more pressing. The Chief Risk Officer (CRO) opened the session by emphasizing the need for a proactive approach to cybersecurity. He invited the Chief Information Security Officer (CISO) to brief the team on how the e-commerce subsidiary could enhance its network security to prevent DoS attacks and unauthorized access. The CISO suggested implementing stateful inspection to monitor network traffic dynamically, while the Chief Technology Officer (CTO) argued that proxy-based filtering would provide greater control over outbound traffic. The discussion revealed that a hybrid approach, combining multiple filtering techniques, would likely provide the best balance between security and performance.

The conversation naturally evolved to secure remote and hybrid access for employees across both entities. The Head of IT Security explained that traditional VPNs were proving insufficient in handling diverse access points, and the company was considering a shift toward zero-trust architecture. The committee discussed the benefits of identity and access management solutions, including multi-factor authentication and role-based access controls. The Chief Human Resources Officer (CHRO) raised concerns about the impact on employee productivity, prompting a debate on how to maintain a seamless user experience while ensuring robust security. Endpoint security for personal devices also emerged as a critical topic, with the Risk Management Committee stressing the importance of strict policies and cybersecurity awareness programs.

Midway through the session, the discussion shifted to a recent cybersecurity breach at competitor fintech company, where sensitive customer data had been compromised. The Compliance Officer reminded the leadership team of their obligation to report such incidents to the national cybersecurity response agency, warning that non-compliance could lead to penalties and reputational damage. The CRO questioned whether the Company's security policies were sufficiently proactive or merely reactive. The consensus was that investing in continuous threat monitoring and incident response mechanisms was essential to prevent future breaches.

Attention then turned to risk management at the multinational level. The fintech company was rapidly expanding its operations, and the committee recognized the need for a globally recognized cybersecurity framework. The CIO emphasized the importance of prioritizing investments in cybersecurity infrastructure based on critical operational risks. The team explored strategies for integrating cybersecurity risk management with business objectives, ensuring that investments in cybersecurity were both effective and cost-efficient. The discussion underscored the significance of aligning cybersecurity strategies with regulatory requirements across different regions, ensuring compliance while optimizing security practices.

Further complicating matters, one of the firm's major financial clients faced increasing cyber threats, including phishing, ransomware, and identity fraud. The firm was engaged in helping this client develop a robust Cyber Crisis Management Plan (CCMP) that aligned with regulatory frameworks and RBI guidelines. Cybersecurity and regulatory teams worked closely with the client to integrate proactive threat detection, swift incident response strategies, and effective recovery protocols. The firm also advised on fostering a cybersecurity-conscious corporate culture to minimize risks associated with human error.

As the meeting neared its conclusion, a critical issue surfaced concerning the e-commerce subsidiary. The platform had come under legal scrutiny for allegedly enabling the sale of counterfeit products. While the Company claimed intermediary protection from liability, legal experts pointed out that this protection was contingent on demonstrating due diligence. The discussion revolved around the necessary steps the e-commerce platform should take, including setting up automated monitoring tools, strengthening seller verification processes, and swiftly acting on customer complaints regarding counterfeit goods. The committee emphasized that beyond legal compliance, ensuring a trustworthy platform was essential for maintaining customer confidence and long-term sustainability.

In the light of above case scenario, answer the following questions :

(*a*) How should the e-commerce subsidiary of both Paythen Ltd and Kyuthen Ltd optimize network security using hardware as well as software or combination of both to prevent DoS attacks and unauthorized access while maintaining efficiency ?

(*5 marks*)

(*b*) Explain the key components of a Cyber Crisis Management Plan and outline its significance in mitigating cyber risks for financial institutions.

(*5 marks*)

(*c*) How should the Paythen Ltd respond to a cybersecurity breach while ensuring regulatory compliance and strengthening its cyber resilience ? Name and state the role of national nodal agency in this regard.

(*5 marks*)

(*d*) What measures should Paythen Ltd implement to enhance cybersecurity resilience and protecting critical infrastructure to manage risks effectively across its operations and supply chain ?

(*5 marks*)

(*e*) Explain the method which the e-commerce subsidiaries of fintech companies Paythen Ltd and Kyuthen Ltd should use to navigate legal risks related to counterfeit products while ensuring responsible platform management.

(*5 marks*)

3. In a recent strategic management meeting held at Sainik Enterprises Ltd, a medium-sized enterprise operating in the precision engineering sector, senior management engaged in an intensive discussion regarding the Company's technology infrastructure and its preparedness for future growth. The enterprise had witnessed commendable expansion over the past five years, extending its market presence significantly within India and internationally. However, operational bottlenecks, fragmented data management systems, and escalating cybersecurity concerns had surfaced, compelling the leadership to critically evaluate the existing technological framework.

During the meeting, Priyank Sharma, the Head of IT and Data Security, highlighted an alarming incident that had recently shaken the confidence of enterprises nationwide. In one highly publicized cybercrime case, an employee at an Indian call center misused confidential credit card details of an international customer to conduct unauthorized online transactions. The incident not only

led to severe reputational damage but also resulted in India's first conviction for cybercrime involving the misuse of foreign customers' data. Drawing parallels, Priyank emphasized the critical importance of strengthening internal data governance and robust cybersecurity practices. Her concern was compounded by the increasing reliance on cloud-based services, which, despite their operational benefits, inherently heightened risks associated with data breaches and insider threats.

Adding to the complexity, Anita Kar, the Chief Operations Officer, steered the discussion towards the Company's immediate need for a comprehensive Enterprise Resource Planning (ERP) system. He argued that fragmented legacy systems were creating inefficiencies, inaccurate forecasting, and inventory mismanagement. According to Anita, investing in an ERP solution was vital not only for integrated management of core business processes but also for enhancing real-time visibility across departments, enabling informed decision-making. Nevertheless, the management acknowledged that selecting an ERP system required meticulous evaluation, balancing cost constraints, necessary functionalities', and vendor reliability. It was clear from previous internal assessments that indiscriminate ERP adoption without thorough due diligence had led competitors into financial overruns and operational setbacks. Ananda Menon, the Finance Head, echoed the cautious sentiment, emphasizing the necessity of a structured evaluation framework before committing significant capital investment into any ERP solution. He stressed the importance of clearly defining organizational objectives, involving cross-functional teams in the evaluation,

and conducting thorough vendor assessments to measure reliability, support capabilities, and scalability. The evaluation process, according to Anand, must incorporate comprehensive cost-benefit analysis, encompassing not just the initial implementation but ongoing maintenance, training, and support.

Raken Joshik, Head of Business Analytics, seized upon this moment to highlight how contemporary ERP solutions were increasingly integrating artificial intelligence (AI) and machine learning (ML), offering significant potential to enhance strategic and operational decision-making capabilities. He explained that leveraging AI-driven ERP systems could automate routine tasks, optimize inventory management through predictive analytics, and significantly improve demand forecasting accuracy. Raken advocated for a strategic approach to integrating AI capabilities within ERP systems, emphasizing that intelligent data analysis could lead to more accurate and quicker managerial decisions, operational optimization, and considerable cost savings. However, Smritina Iyer, Head of Procurement and Logistics, cautioned against over-reliance on technology without clearly defining management practices. She argued that although AI and automation were beneficial, the role of Management Information Systems (MIS) should not be underestimated. Smritina advocated for a balanced approach, suggesting organizations should utilize expert systems for specific diagnostic and problem-solving tasks. Her recommendation aimed at ensuring a smooth synergy between technological adoption and human managerial oversight, thereby preventing over-automation that could potentially obscure managerial judgment and responsiveness.

Rajivan Nair, Chief Technology Officer, further enriched the discussion by addressing the contemporary shift towards Software-as-a-Service (SaaS) models. He acknowledged the notable

advantages of SaaS, such as reduced upfront capital expenditure, scalability, and enhanced flexibility, particularly beneficial for SMEs like Sainik Enterprises. Nonetheless, Rajivan underscored the potential challenges accompanying SaaS adoption. Rajivan recommended adopting a strategic SaaS integration approach by carefully assessing the reliability of vendors, negotiating robust Service Level Agreements (SLAs), and ensuring stringent cybersecurity measures are embedded within service contracts.

Concluding the comprehensive deliberation, senior management agreed on establishing a cross-functional task force responsible for formulating a detailed strategic roadmap. The aim was to ensure an informed, balanced, and future-proof technological infrastructure capable of supporting sustained organizational growth, enhancing operational efficiencies, and maintaining robust data security.

In the light of above facts, answer the following :

(*a*) Outline the significance of India's first cybercrime conviction that Priyank Sharma, the Head of IT and Data Security revealed in the meeting. Indicate how the case demonstrated the applicability of the Indian Penal Code in tackling online fraud ?

(*5 marks*)

(*b*) Enumerate the approach that Anita Kar the Chief Operations Officer emphasized that businesses should take to structure a thorough evaluation process for identifying the most suitable ERP system while balancing cost, functionality, and vendor reliability.

(*5 marks*)

(*c*) Raken Joshik, Head of Business Analytics emphasized that organizations strategically leverage AI-powered ERP solutions to enhance decision-making, optimize operations, and drive efficiency in key business functions. Explain significant benefits for businesses which AI can deliver ?

(*5 marks*)

(*d*) Smritina Iyer, Head of Procurement and Logistics recommendation aimed at ensuring a smooth synergy between technological adoption and human managerial. Explain the various information systems which are part of MIS contributing to enhance managerial decision-making and operational efficiency.

(*5 marks*)

(*e*) Raken Joshik, Head of Business Analytics, addressed the contemporary shift towards Software-as-a-Service (SaaS) models. Suggest how can companies strategically adopt SaaS solutions to enhance flexibility and cost-efficiency while mitigating concerns around internet dependency and data security ?

(*5 marks*)

4. Zindan Ltd, a leading e-commerce and financial services company, has been experiencing rapid growth, driven by its vast customer base and increasing data volumes. However, the Company faces several challenges across different aspects of its operations, ranging from leveraging data analytics for business insights to ensuring cybersecurity compliance and optimizing its IT infrastructure. As part of its strategic initiatives, the Company's leadership convened a management-level meeting to discuss these critical areas and develop a cohesive plan to address them.

One of the primary concerns raised in the meeting was the effective utilization of customer data. The Company has been collecting extensive datasets, including purchase history, browsing behaviour, demographics, and feedback. However, the challenge lies in deriving actionable insights from this data to improve customer experience and drive sales. The data analytics team proposed implementing data mining techniques to identify patterns and develop predictive models that can forecast customer behaviour. However, the team also highlighted potential challenges, such as ensuring data accuracy, handling missing values, and dealing with inconsistencies that could skew analytical results.

In addition to its e-commerce operations, Zindan Ltd also operates in the financial services sector, handling sensitive customer information, including financial transactions and personal details. The Business Head from the e-commerce operations added a perspective about the challenges the financial services sector was facing. The discussion then moved to a crucial issue—data recovery and business continuity. The IT director highlighted the vulnerabilities businesses face due to hardware failures, cyberattacks, or accidental deletions. The team debated the effectiveness of software-based and hardware-based recovery techniques. Software-based recovery tools were seen as cost-effective solutions for minor data losses. However, in cases of severe hardware failure, the reliance on specialized hardware-based recovery solutions was deemed essential. The risk of operational downtime and potential loss of critical business information emphasized the necessity of robust data recovery protocols.

Another pressing issue was the Company's IT infrastructure. Historically, Zindan Ltd relied on on-premises software for its core operations, ensuring full control over security and system management. However, as data volumes increased, so did the costs of maintaining on-site infrastructure. The IT department proposed transitioning to a hybrid IT model, integrating cloud-based solutions while retaining critical applications on-premises. The leadership team debated the advantages and risks of this transition, with concerns raised about integration complexity, compliance challenges, and potential security vulnerabilities. Beyond operational concerns, Company's legal research division explored innovative ways to enhance legal analysis using computational methods. Traditionally, legal researchers manually analyzed historical court proceedings through intensive reading and note-taking. However, the team was proposing to use data analysis for its research purpose. While some experts cautioned against over-reliance on data analysis without qualitative legal interpretation. Challenges such as citation inconsistencies and the need for structured legal data were also discussed.

As the meeting concluded, the leadership team outlined key questions that needed to be addressed moving forward.

In the light of above case scenario, answer the following questions :

(*a*) As a data analyst at Zindan Ltd, how would you justify that data mining techniques rnay be used to build a predictive model that identifies repeat customers ?

(*5 marks*)

(*b*) *"One of the primary concerns raised in the meeting was the effective utilization of customer data."* Outline the steps involved in the process of data analytics method to ensure the dataset is ready for meaningful analysis.

(*5 marks*)

(*c*) As an IT consultant, list the advantages and challenges of maintaining an on-premises software environment for Zindan Ltd while transitioning to a hybrid IT model.

(*5 marks*)

(*d*) Enumerate the key steps that Zindan Ltd should take to implement robust data recovery protocols in cases of severe hardware failures or data corruption incidents.

(*5 marks*)

(*e*) As a legal data analyst, explain the role of network analysis in legal history research and outline its applications in analyzing court proceedings.

(*5 marks*)

———— o ————