IMPACT OF CYBERCRIME ON THE ONLINE BUSINESS AND DIGITAL TRANSITIONS IN THE MODERN ERA

Anurag Gourav[*] Dr. Vinod Kumar Saroj[*] Dr. Sanjai Kumar Singh[*]

INTRODUCTION

The rapid growth of online commerce and computerised trade has transformed global trade, bringing with it new opportunities and challenges for buyers, sellers, governments, and organisations. With the entire economy shifting online in India due to the pandemic, the internet industry has generated enormous profits. The majority of people who play video games today reside in Asia, where the industry is valued at billions of dollars. With computerised education, an advanced economy, and telecommuting, everything moved online overnight, which contributed to a spike in cybercrime cases in India. Indian users' data is misused, and there is a lack of suitable digital regulations covering protection; more than half of the population lost private information online, and there have been cases of credit and debit card fraud, as well as online job fraud. India's digital regulations need to be changed so that cyberwarfare and phishing are subject to harsh penalties. In India, because of the weak network security framework and shaky digital regulations that have affected the economy, banks are vulnerable to cybercriminals. People have lost thousands of dollars in just a few months. India also has to get knowledgeable in this area and update its digital protection plan.

As more and more things in India are being done online and the country becomes more digitalised, the number of cybercrimes is increasing. Indians, especially those who reside in semi-rural and rural areas, as well as the elderly population, need internet knowledge. India has suffered numerous cyberattacks; as of yet, there is no proper legislation providing protection. We need to update the cyber law, which currently gives the notion of cyberspace the utmost importance, impacting both national security and the Indian economy. Cybersecurity should be the main focus of laws. Since cyberspace is the future of the world and everything will soon be

[*]RESEARCH SCHOLAR, NARAYAN SCHOOL OF LAW, GNSU, JAMUHAR, BIHAR.
[*]PROFESSOR, NARAYAN SCHOOL OF LAW, GNSU, JAMUHAR, BIHAR.
[*]ASSOCIATE PROFESSOR, NARAYAN SCHOOL OF LAW, GNSU, JAMUHAR, BIHAR.

digitised, our country needs more cyber experts. College and university courses, as well as school chapters, should deeply consider cybercrime and cybersecurity. This essay examines the various ways that cyber legislation affects digital transactions and e-commerce. Through an extensive literature review, an analysis of the function of regulatory frameworks, and case studies, the study explores how cyber laws influence consumer perception, influence business practices, and lessen the risks associated with online transactions. Important findings emphasise the fundamental role that cyber laws play in fostering a safe and supportive e-commerce ecosystem by coordinating development with regulatory compliance. The examination of challenges, including jurisdictional difficulties, cross-border exchanges, and emerging innovations, highlights the need for adaptable regulatory mechanisms to handle the growing risks and opportunities in the digital economy. At the conclusion, the paper shares insights into how cyber law is evolving and what it means for e-commerce stakeholders.

EVOLUTION OF DIGITAL PAYMENT AND ITS USES IN E-COMMERCE

E-commerce is defined by the Organisation for Economic Cooperation and Development (OECD) as a 'new form of doing business that occurs across networks that employ non-proprietary protocols developed through an open standard-setting process such as the Internet.'[1] E-commerce, as defined by the FDI Policy, includes both digital and physical items as well as services transacted via digital and electronic networks.[2] Online purchases can be performed directly through the website or through affiliates or agents. Selling online can be done through social networking sites, auction websites, or your own website. In terms of business technology, the growth of e-commerce has created a marketplace for the purchase and sale of goods as well as fueled vital internal corporate processes. Financial institutions have also provided their clients with a wide range of cutting-edge services, the most popular of which are digital payment solutions, by utilising information and communication technologies (ICTs). The term "digital financial transactions" (DFTs) has been defined in a number of ways in the past, but the general idea is that DFTs are any financial or payment transactions that involve the use of an electronic or digital device to initiate, activate, and confirm the transaction.[3] All forms of financial transactions conducted through digital or electronic channels, including

[1] Priyanka Barik, D. Sumnath, 'Cyber Law's Emerging Role In Indian E-Commerce' (*KSANDK*, 4 Jan 2022) <https://ksandk.com/regulatory/indian-e-commerce-law-under-cyber-law/#:~:text=Regulatory%20Framework%20For%20E-Commerce%20In%20India:> accessed 10 October 2024

[2] ibid

[3] K. Kajol, Ranjit Singh, Justin Paul, 'Adoption of digital financial transactions: A review of literature and future research agenda' (2022) Technological Forecasting and Social Change <https://www.sciencedirect.com/science/article/pii/S0040162522005121 > accessed 10 October 2024

electronic payments, mobile wallets, cryptocurrency, and online payments, are categorised as DFTs.[4] The way we perform financial transactions has been completely transformed by digital payments, which are now quicker, more convenient, and available to a wider audience. The environment surrounding digital payments has changed dramatically over time due to both shifting consumer preferences and technological advancements. This piece will take the reader on a historical tour as we examine the full development of digital payments, from their modest origins to the present day of frictionless transactions.

The Emergence of Credit and Debit Cards: The introduction of credit and debit cards marked a critical turning point in the development of digital payments. The first credit card was introduced in the late 1950s, enabling customers to make purchases using credit.[5] Debit cards became more and more common over time, making it possible to make direct bank account payments. Electronic fund transfers (EFTs) marked the beginning of the digital payment journey. A secure messaging system was introduced in the 1970s by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to help financial institutions exchange payment instructions.[6] The internet's introduction in the 1990s made online banking and e-commerce possible. Banks began providing online banking so that clients could view their accounts and make payments. The emergence of e-commerce platforms gave companies a way to market their goods and take online payments. Digital wallets and mobile payments became popular as smartphones became more widely used. Innovative solutions were introduced by companies such as Apple, Google, PayCircle, and PayPal, enabling users to securely store their payment information and make purchases with a simple tap or scan. The early 2010s saw a rise in the use of contactless payments, which are enabled by near field communication (NFC) technology.[7] Tapping or waving a card or smartphone close to a payment terminal provides a smooth and practical way to make payments.

David Chaum introduced the first digital payment system, known as "Ecash," in 1997.[8] It made it possible for users to transact online in secret. However, the system failed to gain much traction due to technical difficulties and regulatory hurdles. Paypal first appeared as a substitute

[4] ibid
[5] 'The Evolution of Digital Payments: A Comprehensive Timeline' (*PayCircle*) < https://paycircle.io/the-evolution-of-digital-payments-a-comprehensive-timeline/ > accessed 12 October 2024
[6] ibid
[7] ibid
[8] Salomon Kisters, 'The Evolution of Digital Payments: A Timeline' (*Originstamp*, 2 June 2023) < https://originstamp.com/blog/the-evolution-of-digital-payments-a-timeline/ > accessed 10 October 2024

for conventional payment methods like checks and money orders in 1998.[9] With an email address and a connected bank account or credit card, users could send and receive money online. The idea of decentralised digital currencies was introduced by the rise of cryptocurrencies like Bitcoin. Cryptocurrencies, which were decentralised and not dependent on established financial institutions, provided a transparent and safe means of conducting transactions thanks to blockchain technology.[10] Digital payment systems have incorporated biometric authentication techniques, such as facial recognition and fingerprint authentication, to improve security and convenience.[11] These developments expedited the authentication procedure and added a degree of security.

DEVELOPMENT OF DIGITAL TRANSACTIONS AFTER DEMONETIZATION IN INDIA

In addition to having a major effect on the economy, India's demonetization policy hastened the country's transition to digital payments. In India, digital payments made up only 10% of all transactions before demonetization; however, in the years since, that percentage has increased to over 20%.[12] The Indian Prime Minister, Shri Narendra Modi, declared on November 8, 2016, that all Rs. 500 and Rs. 1,000 notes—which made up 86% of the country's currency—would be demonetised.[13] The aggressive promotion and adoption of the digital ecosystem in India can be attributed to this strategic movement. A multitude of factors, such as the government's drive towards digitalisation, the rise in e-commerce, and the increase in internet and smartphone penetration, have contributed to the growth of the digital ecosystem in India. Through several programs, including Made in India, Startup India, and Digital India, the Indian government has been aggressively encouraging the use of digital technologies.[14]

Due to a mix of government initiatives, rising internet and smartphone usage, and the growth of e-commerce, the digital payments ecosystem in India has also expanded significantly in recent years. The introduction of the Bharat Interface for Money (BHIM) app, which streamlines digital transaction processing, and the Unified Payments Interface (UPI), which

[9] ibid
[10] 'The Evolution of Digital Payments: A Comprehensive Timeline' (*PayCircle*) < https://paycircle.io/the-evolution-of-digital-payments-a-comprehensive-timeline/ > accessed 12 October 2024
[11] ibid
[12] Inder Pal Singh Sethi, 'Digital Payments driving the growth of Digital Economy' (*National Information Centre*) <https://www.nic.in/blogs/digital-payments-driving-the-growth-of-digital-economy/> accessed 10 October 2024
[13] ibid
[14] ibid

enables real-time interbank transactions, are two important initiatives. Since the National Payments Corporation of India (NPCI) launched UPI (Unified Payments Interface) in 2016, the country has seen a considerable increase in its use.[15] Since the National Payments Corporation of India (NPCI) launched UPI (Unified Payments Interface) in 2016, the country has seen a considerable increase in its use. 2017 saw a YoY growth of 900% for UPI, handling over 100 million transactions worth INR 67 billion.[16] At the end of the calendar year 2022, UPI's total transaction value stood at INR 125.95 trillion, up 1.75 X year-on-year (YoY), as per the NPCI.[17] It's interesting to note that in FY22, the total value of UPI transactions represented almost 86% of India's GDP.[18] It is important to note that in December 2022, payments made to merchants (P2M) accounted for 14.57% of all P2P transactions, and 3.24% of all P2P transactions.[19] More small merchants are using UPI, as evidenced by the increase in smaller transactions that was more noticeable in P2M transactions.

By the end of 2023, there will have been 83.75 billion transactions made through UPI.[20] The National Informatics Centre, Ministry of Electronics & Information Technology, Government of India, developed the DigiDhan Dashboard Application as a platform to track and monitor the use of digital payments in the nation. The dashboard offers up-to-date information on the quantity and value of digital transactions, in addition to details on the different kinds of transactions and the platforms that are being utilised. The following are some of Digidhan Portal's key features: Data on digital transactions in real time: the dashboard breaks down the quantity and value of digital transactions occurring nationwide by category (e.g., credit card, debit card, UPI, etc).[21] Details about the platforms being used: the dashboard offers information on the different e-wallet, BHIM, and UPI platforms that are being used for digital transactions. State-specific data: The dashboard lets users see the amount of digital penetration in various

[15] Inder Pal Singh Sethi, 'Digital Payments driving the growth of Digital Economy' (*National Information Centre*) <https://www.nic.in/blogs/digital-payments-driving-the-growth-of-digital-economy/> accessed 12 October 2024
[16] ibid
[17] Hemant Kashyap, 'Record-Breaking Numbers Of UPI In 2022 Hint At India's Maturing Digital Payments Ecosystem' (*INC42*) <https://inc42.com/features/record-breaking-numbers-upi-2022-hint-india-maturing-digital-payments-ecosystem/ > accessed 12 October 2024
[18] ibid
[19] ibid
[20] 'Total Digital Payments Transactions' (*DigiDhan*) < https://digipay.gov.in/dashboard/default.aspx > accessed 13 October 2024
[21] ibid

areas by displaying the quantity and value of digital transactions occurring in each of India's states.[22]

Transaction History: Users can view their previous transactions by accessing their individual transaction histories through the dashboard.

Reports: A variety of reports, including those on transactions, merchants, and users, are also available on the dashboard.

EFFECT OF CYBERCRIME ON DIGITAL TRANSACTIONS AND BUSINESS

The rapid advancement of technology has had a profound impact on how people interact, transact business, and obtain information. One of the more recent criminal activities brought on by this digital transformation is cybercrime, as it is commonly known. India's increasing digital landscape and internet penetration have made it a prime target for cybercriminals. Understanding the scope and nature of cybercrime in India, as well as the challenges of obtaining electronic evidence, is essential to effectively countering this threat.[23] The cornerstone of India's legal framework for combating cybercrime is the Information Technology Act of 2000 (IT Act). The Information Technology Act delineates the legal parameters for countering cybercrimes and prescribes penalties for transgressions such as unapproved entry, theft of data, and offences pertaining to computers. According to the Reserve Bank of India's (RBI) annual report released on Thursday, digital payment fraud in India has experienced a startling surge, more than fivefold to a record 14.57 billion rupees ($175 million) in the fiscal year ending March 2024.[24] This concerning rise is occurring at the same time that India is quickly becoming a global leader in digital payments, thanks to the extensive uptake of the Unified Payments Interface (UPI) since its 2016 introduction. According to RBI data, UPI transactions have grown dramatically over the last two years, rising 137% to a startling 200 trillion rupees.[25]

---

[22] ibid

[23] Dr. G. Anitha Rathna, Dr. M. Sumathy, Ms. Sneha Jayalakshmi. J 'Cyber Crime And Digital Payments In India: A Comprehensive Analysis' (2023) Conf. Vision For Vishwa Guru India: Initiatives For Global Leadership By 2047 <https://www.researchgate.net/publication/375555213_Cyber_Crime_and_Digital_Payments_in_India_A_Comprehensive_Analysis> accessed 10 October 2024

[24] Pranav Dixit, 'Digital payment frauds surge in India as UPI transactions skyrocket: RBI report' *Business Today* (New Delhi, 1 June 2024) < https://www.businesstoday.in/technology/news/story/digital-payment-frauds-surge-in-india-as-upi-transactions-skyrocket-rbi-report-431695-2024-06-01> accessed 10 October 2024

[25] ibid

The National Crime Records Bureau (NCRB) reports that 4,850 cybercrimes in India in 2023 resulted in a startling loss of ₹66.66 crore.[26] According to a recent report by the Indian Cybercrime Coordination Centre (I4C), over the last three years, digital financial frauds have cost an astounding ₹1.25 lakh crore.[27] The National Cybercrime Reporting Portal (NCRP) states that victims of digital financial fraud reported losing at least ₹10,319 crore in 2023.[28] In its report on "cyber security and rising incidents of cyber/white collar crimes," the Parliamentary standing committee on finance stated that the amount of domestic fraud reported by the SE (Supervising Entities) in FY'23 was ₹2537.35 crore.[29] The report states that 6.94 lakh complaints were received in 2023 alone.[30]

INFORMATION TECHNOLOGY ACT, 2000 AND OTHER RELATED LEGISLATION TO CONTROL CYBER CRIME

The first e-commerce legislation passed by the Indian government was the Information Technology Act of 2000. Giving effect to the 1996-published UNCITRAL Model Law on Electronic Commerce (E-Commerce Law) was the main goal of this legislation.[31] The Act addresses data theft, computer damage, and unauthorised access.[32] It offers legal remedies and sanctions for offences involving illegal access to computer systems, computer contamination, and unlawful data extraction. The Information Technology Act 2000 addresses a number of cybercrimes, including identity theft, hacking, and cyber fraud. It gives law enforcement organisations the authority to look into and bring charges against anyone responsible for these offences.[33] In the interest of India's sovereignty or integrity, defence, security, friendly relations with other states, public order, or to stop incitement to commit any cognizable offence or to investigate any offence, the act gives the authorities the authority to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource.[34]

---

[26] Bharat Reddy, 'Digital financial frauds in India: a call for improved investigation strategies' *The Hindu* (New Delhi, 25 March 2024) < https://www.thehindu.com/sci-tech/technology/digital-financial-frauds-in-india-a-call-for-improved-investigation-strategies/article67988607.ece > accessed 12 October 2024
[27] ibid
[28] ibid
[29] Bharat Reddy, 'Digital financial frauds in India: a call for improved investigation strategies' *The Hindu* (New Delhi, 25 March 2024) < https://www.thehindu.com/sci-tech/technology/digital-financial-frauds-in-india-a-call-for-improved-investigation-strategies/article67988607.ece > accessed 11 October 2024
[30] ibid
[31] Priyanka Barik, D. Sumnath, 'Cyber Law's Emerging Role In Indian E-Commerce' (*KSANDK*, 4 Jan 2022) <https://ksandk.com/regulatory/indian-e-commerce-law-under-cyber-law/#:~:text=Regulatory%20Framework%20For%20E-Commerce%20In%20India:> accessed 10 October 2024
[32] Information Technology Act 2000, s 43
[33] Information Technology Act 2000, s 66
[34] Information Technology Act 2000, s 69A

The same provision was used as justification for the recent prohibition of some Chinese apps.[35] To forbid unfair business practices in e-commerce, protect the interests of consumers, and ensure that e-commerce platforms are transparent, these new regulations of consumer laws have been enforced in accordance with the Consumer Protection Act of 2019.[36]

The Computer Emergency Response Team (CERT-In) was created as the administrative body in charge of gathering, analysing, and sharing data on cybersecurity incidents, as well as implementing emergency response measures by the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.[37] In addition, intermediaries and service providers are required by these regulations to notify the CERT-In of cybersecurity incidents. Companies that process, collect, store, or transfer sensitive personal data or information are required to put reasonable security practices and procedures in place under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI rules).[38]

Information Technology Intermediary Guidelines (Amendment) Rules, 2018: In accordance with the Act, the Rules have been developed.[39] The topic of intermediary liability is covered here. As per the legislation, intermediates are required to exercise due diligence in the performance of their duties and to adhere to any additional guidelines that may be specified by the Central Government.[40] Enacted in 2023, the Digital Personal Data Protection Act: The Minister of Electronics and Information Technology introduced the Digital Personal Data Protection Bill, 2023, in the Lok Sabha on August 3, 2023.[41] The mentioned Act was passed by the Parliament on August 7, 2023, and unanimously approved by the Rajya Sabha on August 9, 2023. On August 11, 2023, the bill was ratified by the President.[42]

Processing is the act of carrying out a series of operations on digital personal data, either fully or partially automated. This includes gathering, storing, indexing, sharing, using, disclosing,

[35] Information Technology Act 2000, s 69A
[36] Regulations for Consumer Protection (E-Commerce Law), 2020
[37] Nehaa Chaudhari, 'A comparison of cybersecurity regulations: India' (2022) Asia Business Law Journal < https://law.asia/india-cybersecurity-regulations-2022/ > accessed 15 October 2024
[38] ibid
[39] Information Technology Act 2000, s 79
[40] Information Technology Act 2000, s 79(2)(c)
[41] Ishwar Ahuja, Sakina Kapadia, 'Digital Personal Data Protection Act, 2023 – A Brief Analysis' *Bar and Bench* (New Delhi, 24 August 2023) < https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis > accessed 11 October 2024
[42] Ibid

disseminating, and erasing the data.[43] Only "lawful purposes"—those for which a data principal has granted consent—and specific, Act-defined legitimate uses are eligible for this kind of processing. Consent: The Act stipulates that Personal Data may only be processed for the designated purpose and with the Data Principal's (individual's) consent.[44] Such consent must have clear affirmative action and be free, explicit, informed, unconditional, and unambiguous. Penalties: The Act's Schedule part specifies the number of fines that will be applied for different violations and offences against the Act.[45] For example, there is a penalty of (i) INR 200 Crore for not complying with obligations about children; and (ii) INR 250 Crore for not taking security measures to prevent data breaches.[46]

NEW CRIMINAL LAWS AND THEIR IMPLICATIONS ON CYBER AND RELATED CRIMES

It's interesting to note that the recently enacted law uses the term "electronic communication" to identify contemporary channels or instruments utilised by someone who incites or supports separatist sentiments.[47] Concerns regarding online responsibility and privacy are raised by this explicit inclusion of electronic communication in conjunction with recommendations made under the new[48] Telecommunications Act. Cybercrime is classified as an organised crime class under[49] the New Nyaya Sanhita. False information is also illegal to create and publish, according to BNS.[50] Given how broadly these offences are defined, it would be more legally sound to give them specific definitions. It is still unclear how e-commerce and social media platforms will fit into this formulation, as well as how much liability these platforms will be exposed to. It allows for the seizure of any electronic device or record containing digital evidence, and it also allows for the production of such records by people other than the accused. If a police officer has good reason to suspect that a person's property won't be returned without causing undue delay, they may search and seize that person's belongings without a warrant. Given that it is far more likely that electronic devices will be available for seizure in investigations against businesses or corporations, the increased powers at the disposal of law

[43] Ishwar Ahuja, Sakina Kapadia, 'Digital Personal Data Protection Act, 2023 – A Brief Analysis' *Bar and Bench* (New Delhi, 24 August 2023) < https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis > accessed 11 October 2024
[44] Digital Personal Data Protection Act 2023, s6
[45] Digital Personal Data Protection Act 2023, Sch I
[46] Digital Personal Data Protection Act 2023, s8(5)
[47] Bharatiya Nyaya Sanhita, 2023, s 196
[48] Telecommunications Act, 2023
[49] Bharatiya Nyaya Sanhita, 2023, s 111
[50] Bharatiya Nyaya Sanhita, 2023, s 197(d)

enforcement may have significant implications. This raises the risk that multinational corporations' local offices in India will have to take, even in situations where the primary business activity is conducted abroad. This might have an effect on reputation, confidentiality, and business operations. Each state government is required by Section 398 BNSS (the new procedure code) to establish a witness protection program in order to guarantee the safety of witnesses.[51] Digital or electronic records now have the same "legal effect, validity, and enforceability" as physical documents under the New Evidence Code.[52] Electronic communications are also considered records since such records also contain data that is saved, recorded, or copied in a communications device's memory. Section 63 (1).[53]

Theft of Confidential Information: Many organisations store their confidential information on computer systems. In violation of the IT Act as well as Section 324 of the Bharatiya Nyaya Sanhita, 2023, Disgruntled employees, rival businesses, and criminals are after this information.[54] Theft of this data carries a different punishment.

JUDICIAL REVIEW ON CYBERCRIME RELATED TO DIGITAL TRANSACTIONS

In the 2017 case of Google v. Visaka Industries,[55] the Delhi High Court expounded on the intermediaries' legal responsibility under the IT Act. It was established that while intermediaries—like social media platforms or internet service providers—have an obligation to remove user-shared unlawful content, they are not directly accountable for it.

In another incident of Pune Citibank Mphasis Call Centre Fraud, in 2005, US$3,50,000 was fraudulently transferred online to a few fictitious accounts from the Citibank accounts of four US customers. Under the impression that they would be a helping hand to those customers in dealing with difficult situations, the employees won the trust of the customers and obtained their PINs.[56] Rather than cracking passwords or getting past firewalls, they were finding weaknesses in the MphasiS system. The Court noted that the defendants, in this case, are former workers of the MphasiS call centre. The employees there are checked whenever they enter or

[51] Bharatiya Nagarik Suraksha Sanhita, 2023, s 398
[52] Bharatiya Sakshya Adhiniyam, 2023, s 61
[53] Bharatiya Sakshya Adhiniyam, 2023, s 63(1)
[54] Information Technology Act 2000, s 43, s 66B
[55] CR APPL NO. 1987 OF 2014
[56] 'Cyber Crime and Practice'(*The Institute Of Company Secretaries Of India* 2016) < Cyber_Crime_Law_and_Practice.pdf (icsi. https://www.icsi.edu/media/webmodules/publications/Cyber_Crime_Law_and_Practice.pdfedu)> accessed 13 October 2024

exit. It follows that the staff members had to have committed the numbers to memory. The funds were transferred via the Society for Worldwide Interbank Financial Telecommunication, or SWIFT, service.[57] Unauthorised access to the customers' electronic accounts was used to commit the crime. As a result, this case is classified as a "cybercrime." Any offence under the IPC involving the use of electronic documents can be treated on an equal footing with crimes involving written documents because the IT Act is sufficiently broad to cover these types of crimes. The court determined that because of the nature of unauthorised access involved in conducting transactions, section 43(a) of the Information Technology Act, 2000, is applicable. Section 420, i.e. cheating, Sec 465, Sec 467 and Sec 471 of The Indian Penal Code, 1860, and Section 66 of the Information Technology Act, 2000 were also used to charge the defendants.[58]

In Sandeep Vaghese v. State of Kerala[59] an important judgement, a crime was registered against nine individuals, alleging offences under Sections 65, 66, 66A, C, and D of the Information Technology Act, 2000, along with Sections 419 and 420 of the Indian Penal Code. The complaint was filed by the representative of a company that was involved in the trading and distribution of petrochemicals in India and abroad. The business operates a website with the domain name www.jaypolychem.com; however, the first accused, SamdeepVarghese@Sam, who was fired from the company, created another website, www.jayplychem.org, on the internet in collusion with other accused, including Sam's sister and brother-in-law, Preeti and Charanjeet Singh.[60] On that website, malicious and defamatory content about the company and its directors was posted. The accused sister and brother-in-law were residents of Cochin, and they had been conspiring with both known and unknown individuals to defraud the business by engaging in acts of impersonation, forgery, and other crimes. Amardeep Singh and Rahul, along with other accused persons, are accused of damaging the company's and its directors' reputations. The first accused and others sent emails from fictitious email accounts belonging to numerous clients, vendors, banks, and other entities.[61] The Company's name and reputation have suffered greatly as a result of the defamation campaign carried out by all of the aforementioned individuals.

---

[57] ibid
[58] ibid
[59] Bail Appl. No. 2003 of 2010
[60] 'Cyber Crime and Practice'(*The Institute Of Company Secretaries Of India* 2016) < Cyber_Crime_Law_and_Practice.pdf (icsi. https://www.icsi.edu/media/webmodules/publications/Cyber_Crime_Law_and_Practice.pdfedu)> accessed 13 October 2024
[61] ibid

Threat Mail to BSE and NSE Incident: On 19 The first case of cyber terrorism in the state since the Information Technology Act 2000 was amended was filed by the Mumbai police on May 5, 2009.[62] On May 4, 2009, an email containing threats was sent to the BSE and NSE. The Cyber Crime Investigation Cell and the MRA Marg police are working together to investigate the matter. In this case, the suspect is in custody. At approximately 10.44 am on Monday, Shahab Md, whose email address was sh.itaiyeb125@yahoo.in, sent an email to BSE's administrative email address corp.relations@bseindia.com, challenging the security agencies to stop a terror attack, according to the police.[63] The sender's IP address has been linked to Patna, Bihar. Sify is the ISP. Just four minutes before the email was sent, the email ID was created. Two mobile numbers were entered by the sender in the personal details column when creating the new ID. The owner of both numbers is a Patna-based picture frame maker. The MRA Marg police have filed cases for cyberterrorism under the Information Technology Act of 2000, criminal intimidation under the IPC, and forgery with the intent to deceive.[64]

In Sanjay Kumar vs. State of Haryana,[65] Punjab-Haryana High Court judgement, as per the facts, a complaint was filed with the police on February 11, 2003, by the manager of Vijay Bank, NIT, Faridabad.[66] The complaint stated that M/s Virmati Software had assigned the petitioner to maintain the software system that the bank had purchased from them. He was also looking for certain other banks' software systems. The petitioner had access to their computerised accounting system, which allowed them to enter data into ledgers and other accounts, in order to provide these services. It is evident that the learned Appellate court affirmed the upholding of the accused petitioner's conviction under CRR No. 66 of 2013, and that the learned Trial Court was entirely justified in finding the accused petitioner guilty.[67] The petitioner's learned counsel was unable to identify any errors in the lower courts' rulings or misinterpretations of any evidence. Therefore, there is no legal or factual defect in the verdict of guilt rendered against the accused-petitioner, and as a result, this Court's exercise of its

[62] 'Threat mail to BSE puts cops on toes' *Indian Express* (Mumbai, 5 May 2009) <https://indianexpress.com/article/cities/mumbai/threat-mail-to-bse-puts-cops-on-toes/ > accessed 12 October 2024
[63] ibid
[64] 'Cyber Crime and Practice'(*The Institute Of Company Secretaries Of India 2016)* < Cyber_Crime_Law_and_Practice.pdf (icsi. https://www.icsi.edu/media/webmodules/publications/Cyber_Crime_Law_and_Practice.pdfedu)> accessed 13 October 2024
[65] CRR No. 66 of 2013
[66] Anmol Sinha, 'Sanjay Kumar v State of Haryana: An Analysis' (*Lex Quest Foundation*, 15 April 2015) < https://www.lexquest.in/sanjay-kumar-v-state-of-haryana-an-analysis/ > accessed 13 October 2024
[67] ibid

revision jurisdiction is not warranted. Considering the aforementioned, the claims made by the petitioner's learned counsel are without merit. Dismissed in limine.[68]

Another issue related to trademark was raised in D'zine Garage Pvt. Ltd. vs. D'zine Cafe FZE.[69] in the High Court of Madras. The facts were as such that the respondent was using the mark 'D'zine' as a service mark, part of their corporate name, and domain name www.Dzinecafe.com, and the applicant-defendant was being sued by the plaintiff, who is the registered proprietor of the service mark 'D'zine'.[70] The plaintiff filed a lawsuit for permanent injection against the defendant. Respondent argued that the Applicant-Defendant had purposefully adopted a similar service mark/trade name, D'zine café, in an attempt to take advantage of Respondent/Plaintiff's goodwill and reputation to make quick, illegal money without having to put in much work.[71]

In March 2005, the Delhi High Court handed down a landmark ruling in the National Association of Software and Service Companies vs. Ajay Sood & Others case.[72] The court ruled that "phishing" on the internet was prohibited and that damages could be recovered along with an injunction. The defendants ran a placement agency that engaged in recruiting and headhunting. In the name of NASSCOM, the defendants composed and sent emails to third parties requesting personal information that they could use for headhunting.[73] This case sends a clear message to IP owners that they can conduct business in India without compromising their intellectual property rights and confirms their confidence in the ability and willingness of the Indian legal system to uphold intangible property rights.

FUTURE OF DIGITAL TRANSACTIONS AND ITS USES IN BUSINESS

Conversely, open banking standards are a collection of guidelines and technological solutions intended to make it easier for various organisations to share financial data. The goal of open banking is to make it possible for customers to safely and conveniently share their financial

[68] ibid
[69] 2008(36) PTC 614(MAD)
[70] 'Cyber Crime and Practice'(2016) The Institute Of Company Secretaries Of India < Cyber_Crime_Law_and_Practice.pdf (icsi. https://www.icsi.edu/media/webmodules/publications/Cyber_Crime_Law_and_Practice.pdfedu)> accessed 13 October 2024
[71] ibid
[72] 119(2005) DLT596
[73] Aniket Jadhav, 'NASSCOM v. Ajay Sood & Ors' (2020) Nayaysastram < https://www.nyayshastram.com/post/nasscom-v-ajay-sood> accessed 13 October 2024

information with other financial institutions, payment processors, and outside services.[74] The application of biometrics to digital payments is another developing field. Biometric technology identifies and authenticates people based on their physical traits, such as fingerprints or facial recognition.[75] Some banks and payment companies are already using this technology, and in the upcoming years, it is expected to become more widely used.

To facilitate greater cooperation between various payment systems, numerous nations and organisations have created frameworks and initiatives aimed at achieving interoperability and open banking standards. These initiatives include industry-led projects like the Open Banking standard in the UK and regulatory frameworks like the Second Payment Services Directive (PSD2) in the European Union.[76] Lastly, there's a chance that artificial intelligence (AI) will alter how we make payments for products and services. AI is capable of analysing enormous volumes of data and forecasting customer behaviour. This implies that payment processors can design more customised payment experiences for users, resulting in quicker, simpler, and more convenient payments. Digital payments have a promising future thanks to technological developments that will make them safer, more affordable, and faster. The rise of mobile payments, the use of biometrics, the potential of cryptocurrencies, and the power of AI are all contributing to a digital payment revolution.

While researching this paper, I have identified several significant findings about cybercrime and Online business as stated below:

Regulatory Frameworks and Compliance: Cyberlaw frameworks are essential for setting legal parameters and specifications for companies that conduct online sales. Adherence to these standards is crucial in guaranteeing the safety of consumer information, data integrity, and equitable corporate operations.

Consumer Trust and Privacy: By protecting personal data and guaranteeing open handling of information in digital transactions, effective cyber regulations help to improve consumer trust. Regulations about data protection and privacy are essential to creating a safe and reliable online environment.

[74] Salomon Kisters, 'The Evolution of Digital Payments: A Timeline' (*Originstamp*, 2 June 2023) <https://originstamp.com/blog/the-evolution-of-digital-payments-a-timeline/ > accessed 10 October 2024
[75] ibid
[76] *Ibid*

Effect on Business Operations: Companies must adjust to changing cyber law regulations, which present both opportunities and challenges. Investments in cybersecurity defences, legal support, and operational modifications are frequently needed for compliance initiatives in order to reduce legal risk and guarantee regulatory compliance.

Businesses: Upholding operational integrity and customer trust depends on understanding and adhering to cyber law rules. To effectively handle regulatory hurdles, businesses should prioritise investing in cybersecurity measures and legal compliance techniques.

Consumers: Increased legal safeguards provided by cyber law frameworks help to boost customer trust in online transactions. For customers to be empowered to make educated decisions when making purchases online, they must be aware of their rights and safeguards.

Policymakers: They are essential in creating cyber law frameworks that strike a balance between innovation and regulatory supervision. Laws must be continuously updated to reflect new developments in technology and security risks in order to remain relevant and effective.

CONCLUSIONS AND SUGGESTIONS

India has witnessed a sharp rise in the use of smartphones and internet access in recent years, making digital payments more significant there. As a result, the usage of digital payment systems like card payments, UPI, and mobile wallets has significantly increased. The government is attempting to change this by encouraging the use of digital payments, but a sizable portion of the populace still relies on cash transactions. This will be applied to numerous projects aimed at advancing digital payments. Encouraging retailers to accept digital payment methods will be one of the main goals. This could involve tax breaks and subsidies for retailers to buy point-of-sale terminals. Cybersecurity on the network refers to the hardware and software defences against interruptions, unauthorised access, and other misuse of the infrastructure and network.[77] Company assets are protected against a range of attacks from both inside and outside the organisation with the help of robust network security. In the Multiple Factor Verification system, a user cannot access websites or software programs without multi-factor authentication (MFA) until they have successfully presented additional forms of

[77] Dr. G. Anitha Rathna, Dr. M. Sumathy, Ms. Sneha Jayalakshmi. J 'Cyber Crime And Digital Payments In India: A Comprehensive Analysis' (2023) Conf. Vision For Vishwa Guru India: Initiatives For Global Leadership By 2047 <https://www.researchgate.net/publication/375555213_Cyber_Crime_and_Digital_Payments_in_India_A_Comprehensive_Analysis> accessed 10 October 2024

identification to a verification device.[78] Protective shields like Anti-virus, the hardware and software safeguards that protect the network's infrastructure from disruptions, unauthorised access, and other abuses, are collectively referred to as network security. A digital signature attests to the authenticity and integrity of a digital document and can be used as an addition to it or as a biometric. A digital certificate is a document that provides security and verifies the identity of the user.

Besides these new safety measures as discussed above, there are various challenges, as follows;

Complicated Regulatory Norms: Cyber laws and regulations can differ greatly between countries, making it difficult for businesses that operate internationally to comply with them. Managing a variety of legal obligations raises the complexity and expense of compliance.

Quick Technological Advancements: Cyber regulations frequently don't keep up with the rapid evolution of digital technologies. This discrepancy may cause regulatory ambiguity since new technologies like blockchain, artificial intelligence, and the internet of things may outpace existing rules.[79]

Data Privacy Issues: While cyber laws try to protect consumer data and privacy, data misuse and breaches remain chronic concerns. Constant attention to detail and proactive steps to safeguard personal data are necessary for compliance with data protection laws (such as the CCPA and GDPR).[80]

Legal Ambiguity and Interpretation: Different people may interpret cyber laws and legal precedents differently, which can cause uncertainty over compliance standards and enforcement. This uncertainty could lead to legal conflicts, sanctions from the authorities, or harm to the reputation of companies that don't comply.

Enforcement and Jurisdictional Issues: Due to jurisdictional variances and disparities in enforcement capacities between nations, enforcing cyber laws across borders can be difficult. This can make it more difficult for victims to pursue meaningful legal remedies and open doors for cybercriminals.

---

[78] ibid
[79] Charu Singh 'Impact of Cyber Law on E-Commerce and Digital Transactions' (July 2024) Global Journal of Current Research <https://www.researchgate.net/publication/381887137_Impact_of_Cyber_Law_on_E-Commerce_and_Digital_Transactions> accessed 10 October 2024
[80] ibid

Admissibility, privacy, and chain of custody are just a few of the legal and procedural requirements that make the collection and storage of electronic evidence even more difficult. To overcome these challenges, law enforcement agencies need to implement effective plans and leverage tools and techniques from the field of digital forensics. Collaboration between the public and private sectors is crucial to strengthening cybercrime investigation capacities and developing a safe environment for managing electronic evidence. This research paper looked at prominent cybercrime cases and the electronic evidence management associated with them in order to highlight the practical implications of current approaches and identify areas for development. It might also be recommended to improve collaboration, raise awareness and educate people about cybersecurity best practices, and fortify laws that combat cybercrime. To secure India's digital infrastructure, we must understand the nature of cybercrime and the challenges presented by electronic evidence.