JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

RIGHTS OF CONSUMER IN DIGITAL ERA ON E-BANKING AND SCOPE OF DIGITAL FORENSICS IN CYBERSPACE

[1]SHAZILA SHAJAHAN, [2]MD JIYAUDDIN

[1]RESEARCH SCHOLAR, [2]ASSISTANT PROFESSOR
[1]LAW DEPARTMENT
[1]VELLORE INSTITUTE OF TECHNOLOGY CHENNAI,INDIA, [2]NORTHEAST FRONTIER TECHNICAL UNIVERSITY ARUNACHAL PRADESH

Abstract : A bank fraud is a purposeful act by any person in path of a banking transaction or in the books of accounts, which results in unlawful profit to any individual for a temporary or otherwise, with or without any monitory loss to the bank. The expansion of information and communication technology has changed the whole globe into a global village, but it has also created a severe hazard to existing and established banking institutions, which is known Cyber Crimes. The proliferation of computers has posed a variety of challenges to the country legislators and law enforcement organizations. Various records, such as printed records, signed records, original records, and so on, were required by legislative rules. The law of evidence is conventionally based on paper records, which must be proven in court through oral depositions and other types of physical evidence. As more transactions are conducted electronically, it is necessary to have evidence of transactions in order to demonstrate legal rights that flow from and derived from them. The Indian banking industry grappling with issue of proving digital and electronic evidence in a court of law. Cybercrime knows no geographical bounds and can damage any country on the planet. The use of information technology to modify the way people commit crimes; the law should not be a bystander but should adapt to the changing environment. In light of the changing environment, it was necessary to rewrite the existing legislation. The majority of Indian laws are focused on the physical environment, geographical boundaries, tangible papers, and records, and were either founded by British government or adopted after independence within first three decades. Everything is recorded in digits in the digital era, regardless of physical limitations. As a result of these repercussions, tough statutory rules are required to regulate illegal actions in the cyber world and to defend the technological advancement system. Taking legal action against cross-border elements and legal questions of jurisdiction presents a number of difficulties. There are other issues of conflict of laws and practical issues such as gathering evidence, extradition of offenders, and international mutual cooperation among countries involved. Without the cooperation of other countries, no single government can establish laws to combat cybercrime on its own.

Keywords: Cybercrimes, Information Technology, Banking frauds, Cyberspace, Legislation

I. INTRODUCTION

"Our Age of Anxiety is, in great part, the result of trying to do today's job with yesterday's tools- with yesterday's concepts" M. Mcluhan.

The 'e-Revolution' virtually made the entire economic world in cyberspace and this innovative trading universe in the lap of cyberspace is known as the 'Digital Economy'. The digital economy is characterized as an economy accompanied by digital technology such as the Internet, Intranet Computers, Software, and other related Information Technologies. Digital Technology refers to The confluence of computing and communication technologies on the Internet and other networks, as well as the resulting flow of information and technology may be fueling e-commerce and massive management alterations. Cyberspace has put the complete banking industry into the virtual world. Individuals have an extensive variety of avenues to the way in and the Internet, in particular, is an aspect of cyberspace. The Internet is not a corporal or substantial entity, but rather a gigantic network which interconnects inestimable smaller groups of connected computer networks. This e-revolution has strained the banking industry to reorganize, reinvent and advance their products and services as per the need of the hour. Customers or consumers are cherishing most of the benefits of Electronic Banking. E-Banking has developed into part and parcel of our modern life. However, the rights of consumers are not in safe hands. The United Nations Commission on International Trade Law (UNCITRAL), which was established by the United Nations General Assembly in 1996, adopted the Model Law of Electronic Commerce in 1996 in order to balance the growth of e- commerce with international legal standardization and compatibility of practices. It advocated that the usage of e-mail, telegrams, telex, and telegraphy, among other things, develop smoothly by establishing norms whereby their legal worth could be determined. E-banking has evolved into a necessary and long-lasting weapon, reshaping the whole banking industry. Customers can now obtain banking services at a very low cost with a single click of the mouse, as well as a great deal of flexibility in selecting vendors for their financial service needs. Banks must continuously innovate and move forward.

2. PARALLEL GUIDELINES IN THE INDIAN PENAL CODE AND INFORMATION TECHNOLOGY ACT

2.1. Hacking and Data Theft

"Hacking into a computer network, data theft, introducing and spreading viruses through computer networks, destroying computers, computer networks, or computer programmers, disturbing any computer, computer system, or computer network, denying an authorized user access to a computer or computer network, destroying information residing in a computer ", and so on are all forbidden under Sections 43 and 66 of the IT Act. "The penalty for the aforementioned offences are a maximum of three years in prison or a fine of Rs. 5, 00,000 or both". Section 22 of the IPC stated " movable property are proposed to take account of the corporeal property of every description, except land and things attached to the earth or enduringly fastened to anything attached to the earth", Section 378 of the IPC will be relevant to the "theft of any data, online or otherwise"." The maximum penalty for theft under section 378 of the IPC is three years in prison or a fine, or both". Whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or assists in the suppression or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description for a term which may extend to 2 (two) years, or with fine, or with both, according to Section 424 of the IPC. This part will be applicable to data theft. Section 424 carries a " maximum penalty of up to 2 (two) years in prison, a fine, or both". "Whoever, with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person causes the destruction of any property, or any such change in any property or in the situation thereof, as destroys or diminishes its value or utility, or affects it injuriously, commits mischief" according to Section 425 of the IPC. "Damage to computer systems, as well as blocking admittance to a processor arrangement, will come under aforementioned section 425 of the IPC" 10 . "The penalty for mischief under section 426 of the IPC is maximum of three months in jail, a fine, or both".

2.2. Identity Theft and Cheating by Personation

Identity theft is punishable under Section 66C of the IT Act, which state "anyone fraudulently or dishonestly makes another person electronic signature, password, or other unique identification the feature shall be punished with imprisonment of either description for a term that may extend to 3 years, as well as a fine of up to Rs. 1,00,000 person who cheats by personation by using any communication device or computer be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to a fine which may extend to Rs. 1, 00,000." (Rupees one lack). Section 419 of the IPC additionally makes a penalty for "cheating by personation", "anyone who cheats by personation be punished with either imprisonment of any description for a time up to 3 years, a fine, or both." "A person is considered to be guilty of "cheating by personation" " if he or she cheats by claiming to be someone else, or by deliberately substituting one person for another, or by representing himself or herself as someone different than who he or she is". For identity theft, the provisions of sections 463, 465, and 468 of the IPC, which deal with forgery for the purpose of cheating, may also apply. Forgery for the purpose of "defrauding is punishable under Section 468 of the IPC, which stipulates a penalty of imprisonment of any kind for a time up to 7 (seven) years, as well as a fine". Sections 463, 465, and 468 of the Indian Penal Code, which deal with forgery for the purpose of cheating,can taken into consideration in cases of identity theft.

3.DIVERGENCE FLANKED BY CRIMINAL AND TECHNONOLOGICAL LAWS : DISCUSSION OF CASE LAW

When it comes to "Sharat Babu Digumarti v. Government of NCT of Delhi", discrepancy among the IPC and IT Act was brought in light. The facts of case is that , an obscene film was posted for sale on November 27, 2004. To avoid detection by filters, the listing was placed under the category ; and the sub-category. Before the listing was taken down, a few copies were sold. The crime branch of the Delhi police charged Avinash Bajaj's managing director, and Sharat Digumarti, Bazee manager. Because Avinash Bajaj and employer, Bazee, was not named as a defendant, the court ruled that "vicarious liability could not be imposed under either section 292 of the IPC or section 67 of the IT Act". After that, the charges against Sharat Digumarti under section 67 of the IT Act and section 294 of the IPC were withdrawn, but charges under section 292 of the IPC were kept. The Supreme Court next assessed whether a charge under section 292 of the IPC would be persistent after the charges under section 67 of the IT Act were withdrawn. Proceedings against Sarat Digumarti were overturned by the Supreme Court, which found if any violation is committed involved an electronic record, the IT Act will be relevant because that was the legislative objective. It is a well-established tenet of construal analysis that particular laws will win over general laws, and that later laws will overrule earlier legislation. Furthermore, section 81 of the IT Act specifies that provisions of the cyber laws will take "effect notwithstanding
anything in any other law currently in force that is inconsistent with them".
Certain persons accused of stealing data and software from owner and booked under of sections 408 and 420 of the IPC as well as sections 43, 65, and 66 of the IT Act in the case " Gagan Harsh Sharma v. The State of Maharashtra" . With the exception of section 408 of the IPC, all of these sections have already been considered. Criminal breach of trust by clerk or servant is dealt with in Section 408 of the IPC, explains so whoever, being a clerk or servant or employed as a clerk or servant, and being in any manner entrusted in such capacity with property, or with any dominion over property, commits criminal breach of trust in respect of that property, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine". The Indian Penal Code&;s Sections 408 and 420 are non-bailable and can only be considered with approval of court. Sections 43, 65, and 66 provide for bail and the compounding of offences. As a result, the petitioners asked for the IPC charges against them to be dropped and the IT Act allegations against them are interrogated. It was argued, if the Supreme Court Judge&; decision in Sharat Babu Digumarti was adopted, the petitioners could only be prosecuted with equivalent conduct under the IT Act, not the IPC.

4. ROLE OF RBI ON CONSUMER PROTECTION ENVIRONMENT IN INDIAN BANKING SECTOR

4.1. CHARTER OF CONSUMER RIGHTS

Right to fair treatment This right forbids banks from discriminating against consumers based on their gender, age, religion, caste, or physical ability when providing products or services. Banks, on the other hand, can continue to offer customers differing interest rates or goods.;However, the financial services provider may have certain special products that are only available to members of a particular market

segment or may discriminate between its clients based on reasonable commercially acceptable economic underlying principles. Right to Transparency, fairness, and honesty.According to charter, banks must ensure that contracts are crystal unambiguos and easily understood by general public. Banks will be responsible for sending out effective communication. The price of the goods, the customer duties, and the major dangers must all be clearly stated. Any aspects that may be detrimental to the customer should be disclosed to him. Important terms and conditions should be clearly displayed for the customers review.

Right to suitability

Despite a slew of laws, mis-selling allegations continue to plague the distribution industry, notably in the case of life insurance policies. Salespeople are enticed by larger incentives to push products without first determining their suitability for the consumer. With the passage of this charter, such authorities may find it more difficult to sell market-linked insurance products to older residents seeking predictable returns. The charter now requires banks to sell products while considering the needs, financial situation, and knowledge of their consumers.

Right to privacy

Banks have a legal obligation to keep customers; personal information private unless the information is necessary by law or the client has given their approval. The charter specifies that;customers have the right to be protected from all types of communications that infringe on their privacy. Banks also dissents from disclosing personal information to telemarketing organisations or for cross-selling purposes.

Right to Grievance Redress and Compensation

The institutionalisation of Internal Ombudsman process in all public sector, selected private sector and foreign banks in 2015 marked significant step forward in enhancing the grievance redressal mechanism available to bank clients. All scheduled commercial banks (other than Regional Rural Banks) with ten or more banking outlets in India are now covered by the Scheme. The goal of establishing is to ensure that banks provide undivided attention to the resolution of client complaints, and that bank customers obtain a self-governing

5. CONSUMER PROTECTION WITH SPECIAL REFERENCE TO OMBUDSMAN SCHEME

The RBI is the one who appoints the Banking Ombudsman Scheme. The Ombudsman is a main dispute settlement forum. Because it is not constrained by any express requirement or procedural regulation, it makes conclusions based on the facts of the case. The Ombudsman plan covers 27 various aspects of the banking industry, but many more remain unaddressed, necessitating a broadening of the scheme reach. The RBI is in charge of this scheme, which is administered through 15 different offices across the country. The scheme& principal goal is to resolve customer concerns about the bank services. This plan covers all scheduled commercial banks, Regional Rural Banks, and Scheduled Primary Co-operative Banks. Grievances grounds under the Ombudsman Scheme Any complaint relating to later inadequacy in financial services can be obtained and considered by the Banking Ombudsman: denying without adequate causes , of petite quantity of notes utilized for any purpose, and for charging commission for non-approval, exclusive of adequate grounds, of coins tendered and charging commission in reverence thereof; non-payment or holdup in payment of internal remittances; letdown to issue or impediment the problem of draughts, pay orders, etc. failure or hindrance in delays, non-credit of proceeds to parties accounts, on-payment of deposit, or not following of RBI guidelines, if any, appropriate to rate of various types of investments in any savings, current, or other account retained with a bank; grievances from Non-Resident Indians with accounts in India in reference to the refusal to open deposit accounts with bank; objections from Non-Resident Indians with accounts in India in regards to their refusal to open deposit accounts with a bank; complaints from Non-Resident with accounts in India in pertain to the rejection to open deposit accounts without a proper reason; make charges without giving the customer adequate warning and if bank fails to follow those guidelines of Reserve Bank and non compliance by the bank or its branches on credit

operations .

6. SCOPE, FUNCTION AND PROCEDURES IN DIGITAL FORENSICS

Electronically stored data must be constructed in such a way that it remains reliable. This usually requires technically segregating the equipment under investigation so that it cannot be tampered with or corrupted by mistake. Investigators analyze digital copies of storage media in a pristine setting to gather information for a case. Among the instruments utilised in this technique are the Wireshark internet protocol analyzer and Basis Technology;s Autopsy for hard drive investigations. In a legal proceeding, forensics experts report their findings to a judge or jury, who evaluates them to help determine a lawsuit& outcome. In a data recovery case, forensic investigators explain what they were able to salvage from a compromised server. Computer forensic investigations combine a variety of approaches with in-depth understanding. Steganography is the technique for hiding information in any type of digital file, message, or data stream. By evaluating the data hashes included in the file in issue, computer forensic professionals can undo a steganography attempt. 30 Without the assistance of digital artefacts, investigators evaluate and reconstruct digital activity. Artifacts are unexpected data changes that occur as a result of digital processes. A computer is investigated from within the operating system while the computer or device is running, using system tools on the machine. Monitoring a computer system and recollection for segments of files that were eliminated in one area but left remnants on the machine in another is part of this strategy. This is also known as data carving or file carving

7. NEED FOR CYBERSECURITY IN DIGITAL BANKING SECTOR

It is one of the most common threats to banks, in which data is left unencrypted and is promptly exploited by hackers or cybercriminals, resulting in major consequences for the financial institution. All data stored on computers at financial institutions or on the internet must be encrypted in its entirety. Even if your data is taken, it will be impossible for scammers to use it. End-to-end devices, such as PCs and

mobile phones, are commonly used to execute digital transactions and must be secured. If infested with malware, the bank& cyber security could be jeopardised each time they connect to your network. 31 Sensitive data is transmitted through this network, if a user device is infected with malware that protected, the data could be compromised. Many banks and financial institutions use third-party services from outside companies to better serve their consumers. The bank that engaged these vendors, on the other hand, may be badly damaged if they do not have strict Cyber security measures in place. This is one of the more recent cyber-threats that banks must contend with. When a user inputs his or her login credentials, the cybercriminals will take those credentials and utilizes them later. This cyber threat has progressed to the next level, with crooks employing new spoofing techniques.

8. UTILIZATION OF DIGITAL FORENSICS IN CYBER SECURITY

In recent years, forensics professionals have been paying very close attention to cloud computing because it provides a significant pool of resources, a cost-effective solutions, versatility, and extensive storage access. In hybrid, private, and public cloud computing architectures, security databases among several other services, are offered. This application of modern technology scientific concepts, tried-and-true methodologies, and technological practises to report, examine, preserve, collect, and recognize digital data in the cloud. Digital technological improvements have given many conveniences to the cyber security industry, but they have also generated numerous challenges. It is universally believed that cybercrime is meticulously planned. As a result, digital forensics has a multiplicity of issues. As a result of these challenges, a lot of attention has been devoted to it. Traditionally IT infrastructures with on-premises data processing contain an effective internal control incident management mechanism for ensuring maximum security.Despite the significance of digital forensics as a consequence of cybercrime, the field is impeded by a shortage of skilled and knowledgeable forensic officers. There is a paucity of well-trained forensic investigators since digital forensics necessitate technically competent professionals who are authorized and outfitted to present evidence. Due to fierce competition among law enforcement agencies and stringent eligibility requirements, this is the case. Previous skills and understanding should be used to aid in the training of new digital forensic professionals and to foster knowledge sharing among detective agencies. Unfortunately, many digital forensic officers do not document their work or follow legal rules, placing digital forensic investigations in jeopardy. Forensic specialists can deploy digital forensic operations both asynchronously (after a cyber-crime) and strategically (before a cyber-crime) by integrating digital forensics with AI (before a cyber-crime). The reactive capability of intelligent forensics can be understood of as a characteristic of a digital forensic investigation that aids in obtaining a more in-depth understanding of the incidence, which can then be used to assist the digital forensic officer in analyzing the data sources for relevant evidence.

9. CHALLENGES RELATING TO CYBERSECURITY IN DIGITAL BANKING

Public understanding of cyber security is low, and few businesses spend in training and enhancing people overall cyber security awareness. Cyber security is given a low priority, and as a result, it is widely ignored in budgeting. Cyber security remains a low priority for top management, and support for such programs is likewise minimal. This could be because they underestimate the severity of the threats. Identity and access management has long been a crucial component of cyber security, particularly in these times when hackers have the upper hand and only one hijacked credential is required to get access to an organizational network. Although considerable progress has been made in this area, much more efforts are still needed and works to be done. Endpoint security software that concentrates on executable files has begun to be used by cybercriminals to avoid being detected. 36 Mobile phones became the fundamental form of communication for the majority of banking institutions. Every day, the base increases in size, making it a more enticing alternative for exploiters. Mobile phones have become an enticing target for hackers due to the increase in mobile phone transactions. Hackers have identified new ways to exploit social media as more customers use it. Customers who are ignorant of their data are eager to provide it with anyone in order to see which vulnerabilities are exploited by attackers.

10. REMEDIES TO THE CYBERSECURITY IN DIGITAL BANKING

Analytics is a crucial component of maximizing cyber resilience. A new generation of security information and event management has developed, capable of storing and analyzing substantial quantities of security data in real time. The idea of security as an expense must give way to security as a privilege. Only by analyzing and assessing of security concerns and subsequent impact can the true value of security be understood. Banks and other financial institutions must adopt new technologies that can detect and eliminate unscrupulous behaviours and activities. Because data is now stored on a multitude of devices and in the cloud, every system that stores sensitive information must be safeguarded. It is one of the most crucial aspects in which the consumer must be made realize the importance of not giving their banking credentials to everyone. They must inform the Cyber security cell as quickly as possible if they detect anything suspicious in their transactions or bank account. 37 A firewall can effectively protect your computer, but it won't stop an attack unless you run up-to-date anti-virus and anti-malware software. Updating to the most current version of the software helps protect your system from potentially disastrous attacks. Cyber security in digital banking is an issue that must be addressed. The banking industry has become more susceptible to cybercriminal attacks in digitalization has increased. As a consequences, a reliable Cyber security framework is designed that does not adversely impact the security of consumer and financial institution data and resources.

CONCLUSION

Cyber forensics is a contentious issue in today's modern world. All activities relating to a specific circumstance should be estimated to be responsible for in a digital format and archived in properly designated archives for computer forensic investigators. This guarantees the legitimacy of any findings by permitting these cyber security professionals to illustrate when, where, and how evidence was retrieved. The method involves identifying, accumulating, acquiring, preserving, investigating, and presenting digital evidence is known as digital forensics. For digital evidence to be admissible as evidence of law, it must be legitimate. The forensic artifact and techniques used for data (e.g., static or live acquisition) are entirely determined by the device, its operating system, and its security mechanisms. It also allows specialists to evaluate the authenticity of evidence by analyzing dates and times when the investigator's digitally recorded paperwork was retrieved by prospective suspects via external factors. Several international accords pertaining to cyber warfare have been implemented. In terms of technical substance and extent of reportage of criminalization, investigation procedures

and authorities, digital evidence, supervision and risk, and jurisdictions and international cooperation, contemporary multilateral and regional legal instruments, as well as statutory provisions, vary. The geographic scope and applicability of treaties varies as well. This discrepancy renders it incredibly challenging to detect potential, examine, and prosecute cybercriminals, well as to preventing cybercrimes. There must have been safeguards in place to make sure that laws banning Internet access and materials are not misappropriated and are in conformity with the rule of law and human rights. Clarity in the law is necessary in order to guarantee that laws are not required to prohibit access to content in a way that is violation of human rights.

References

B.R. Sharma, Bank Frauds, Prevention and Detection (Universal Law Publishing Co., Delhi, 2nd edn, 2009).

.Brynolfson ., "Consumer Surplus in the Digital Economy: Estimating the Value of Increased Product Variety at Online Book-sellers", Management Science, 15 (2003).

Holt, T. J., and A. M. Bossler, Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Crime Sciences Series. (New York, Routle, 2016).

Manikyam K Sita , Cyber Crime: Law & Policy Perspective (Hind Law House, Pune, 2006).

Pranab Kumar Bhattacharya, "Legal Framework of Electronic Commerce: A Study with Special Reference to Information Technology Act 2000", 54 The Indian Journal of Commerce, 54(2001).

Pandey Ashish , Criminal Detention and Prevention, (JBA Publisher, New Delhi).

Rankin, G.G.;The Indian Penal Code", Law Quarterly Review (1944).

Ratanlal and Dhirajlal. Indian Penal Code, (Lexis Nexis 2020).

Vidya .C, Cyber Crime& Law an Overview, (The ICFAI University Press, 2007).

Waxman Mathew , "Cyber-Attacks and the Use of Force: Back to the Future of Article." 24 Yale Journal of International Law (2011).

Yen Fen Lim, Cyber Space Law: Commentaries and Material, 4 Oxford University Press, New Delhi,2007).