VOLUME 18 ISSN 2456-9704

CRIMINAL THREAT OF CYBER DATA THEFT: AN ANALYSIS UNDER THE INDIAN CRIMINAL LAW

By Aarushi Chopra
From Amity Law School, Noida

Scope of the Research Project

Statement of problem:
This research paper highlights the issue of criminal threat of cyber-crimes with main emphasis on data theft in India and the lack of proper enactments to tackle the technological intricacies which are involved in the same.

Limitations:
Over the span of approving and examining resources that the researcher has depended upon, it has been unequivocally felt that the ambit of this zone of law is developing, particularly in India. In this manner, the researcher has found over the span of searching for data that the data is chaotic and dispersed. The researcher will be dealing with the accessible data to emphasize on the applicable issues relating to the point.

Abstract

With the increase in internet usage, Data has become an important resource that is now a part of our lives. Considering that data is one of the most critical piece of information or an asset for most of the organizations, crimes regarding stealing, hacking, deleting, removing it are prone to happen. a new series of cyber-crime has come up. This has made a new and different kinds of criminals, who plan to exploit the helplessness of computer programs and use it for their very own benefit or just to cause harm. So with the advancement of technology, where almost everything is getting digitized, data theft stays a huge danger to any organization or an individual. Hence, protection of sensitive data it at all cost has become extremely critical and more than any strong antivirus, which works as a preventive measure, what is also required is set of strong enactments to deal with the crimes as and when any organization or an individual faces it. A lot of countries have already come up with specific acts that help protect data like USA (US Privacy Act, 1974), UK (The Data Protection Act, 1984) and Singapore (Personal Data Protection Act, 2012), but India is still lagging behind in this critical areas. This paper intends to specifically focus on how India is dealing with Data theft and whether current Indian laws within the ambit of existing Information Technology Act and the Indian Penal Code have adequate provisions to safeguards organization from becoming victim of data theft.

Introduction

A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era. According to the Economist data is now the most valuable resource in the world, beating oil. It is the key to smooth functionality of everything from the government to local companies.
Without data, progress would halt. 97% of businesses use data to power their business opportunities and 76% of businesses use data as an integral part of forming a business

strategy.[1] The internet is nothing but a compilation of millions of data being searched, saved, transferred, shared, bought, sold everywhere around the globe. Gigantic amounts of information are created each and every day by organizations working together on the web so as to extract value from separating the patterns that represent the moment of truth which make or break their organizations. It is an important weapon for corporates to capture large market share. Data possessed by an organisation includes personal data of clients, confidential data, financial data, in-house information produced over the span of the business, programming, trade secrets, and so forth. So any information/report in an electronic structure is more inclined to theft than any paper document. This is because they are portable and easy to copy. Not only that but the quantity in which it may be stollen is frightening.

With that being said, let's understand the **definition of data.**

"What is Data?"

"Under the IT Act, 2000, 'Data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer"[2]. According to the Personal Data Protection Bill, 2019, "data" "includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means."[3] In simple terms, data is the quantities, characters, or symbols on which actions are performed by a computer, which may be stored and communicated in the form of electrical indicators and recorded on magnetic, mechanical or optical recording media.

Now that we've understood what data means, the next question that arises is **what is data theft?**

"What is Data Theft?"

Data theft in simple terms is an act of illicit/unapproved replicating, taking or removal of confidential, valuable or personal information from an association without its assent or information. It's the act of taking virtual data with an aim to compromise someone's privacy or to procure confidential data. It may be regarding taking or hacking passwords, banking data, personal data of customers, master card data or some other data, for example, trade secrets, source codes, programming, customer database and so forth of significance to any association, or hacking into government databases for taking confidential data and abusing them and a few more in accordance with these.

"Data theft is currently a new era of crime in India as well as everywhere throughout the

[1] Greg Siele, *Data is the world's most valuable resource,* RingLead (April 18, 2020, 3:32 pm), https://www.ringlead.com/blog/data-is-the-worlds-most-valuable-resource/

[2] The IT Act, 2000

[3] Personal Data Protection Bill, 2019 : http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

world. With the sharp ascent being used of web and technology, a new series of cyber-crime has come up. This has made a new breed of criminals, who plan to exploit the helplessness of computer programs and use it for their very own benefit or just to cause harm."

"So with the advancement of computerized data and advanced trade, where our everyday lives are connected to the internet, exchanges based over E-messages and networking sites, e-shopping is the new trend , where organizations are built in a virtual space and everything is digitized, data theft stays a huge danger to individuals."

"The term 'Data Theft' is in reality a misnomer. As per the Indian law, theft must be committed in regard of movable property. Information is anything but a movable property, and consequently the unapproved act of expulsion of information electronically (by method of E-messaging it to oneself or by hacking into a PC framework, for instance) isn't considered as theft. In any case, taking of information is no uncertainty a criminal offense, and is culpable under the law."

"Sec 378 of the IPC, 1860 defines 'Theft' as follow:-

Whoever intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.

Sec 22 of the IPC, 1860 defines 'Movable Property' as follows:-

The word movable property are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth." [4]

Data is commonly stolen:

- By the personnel or the legally binding/administration merchants utilizing it during the course of their official work.
- Through hacking of computer frameworks.

In the principal case, it's advisable that the concurrences with the staff and temporary workers contain appropriate provisions which may build up a breach of trust for unapproved use and access of data. Such understandings should plainly express that there stands an entrustment of data to the parties and that they ought to limit the extension and technique wherein they could manage the data. For instance: If the personnel being referred to has consented to a Non-Disclosure Arrangement (NDA) regarding a particular project and afterward abuses that data by offering it to another person or utilizing it for his/her advantage, at that point he/she can be considered criminally responsible for breaking the terms under the NDA and from that point be seriously punished for the same."

"What is the punishment for Data Theft?"

"The Indian law deals with punishments and penalties for data crimes in the IT Act, 2000, in this manner making a method of redressal for violations attempted with the help of

[4] The Indian Penal Code, 1860 // sec: 22, 378

technology through the web. This Act is the supreme law managing E-commerce and provides punishments for the following:"

- "Unauthorized access of a computer framework,
- Destruction of computer framework programming,
- Unauthorized download or duplicating of data,
- Tampering with computer source codes,
- Hacking into unapproved computer framework,
- Accessing information kept in secured framework and abusing it. secured system data is that data which is expressed by the legislature as secured information,
- Breach of confidentiality and protection of data by a person who has been agreed powers under the IT Act."

"The IPC defines 'theft' and lays down punishments for theft of movable property which consolidates all corporeal property. This clarifies that data, which is impalpable, is beyond the extent of IPC. In any case, if the information is kept in a medium, for instance: floppy disks, CD, pen drives, hard drives, and so forth., and afterward on the off chance that that is taken, at that point the applicable Sec identifying with theft in the IPC can be applied and thusly the blamed will be arraigned in a criminal court and, if proved guilty, will be criminally charged for the same."

"On the off chance that an issue emerges regarding data crime or any cyber-crime connected to misappropriation of information, at that point the affected individual can submit a complaint by method of a criminal complaint and furthermore a civil complaint according to the nature of the crime, within the police station or a cyber cell in their city."

The country's data protection laws mainly consist of:

- A legal arrangement for settlement of compensation for inability to protect sensitive personal data; and
- A criminal arrangement for exposure of private data without the data subject's information, assent or in breach of a contract.

However, both provisions apply as long as there is a outcome of a wrongful gain or loss from such disclosure or breach.

Government-prescribed rules on privacy apply as long as the parties haven't agreed to their own security standards and, even if they do apply, the sole consequence of non-compliance would be payment of compensation if the breach resulted in wrongful gain or loss.

We as of now have a circumstance where an assortment of offenses are penalised by both the IPC and the IT Act, despite the fact that the components of the two offenses are the same. There are exceptionally unobtrusive contrasts in punishments under these Acts, explicitly in viewpoints like whether the offenses are bailable or compoundable or cognizable.

"In the case of *Gagan Harsh Sharma v. The State of Maharashtra*, certain individuals were accused of theft of data and software from their employer and charged under Secs 408 and 420 of the IPC and also under Secs 43, 65 and 66 of the IT Act.

Offences under Secs 408 and 420 of the IPC are non-bailable and cannot be compounded other than with the permission of the court. Offences under Secs 43, 65 and 66 of the IT

Act are compoundable and bailable. Therefore, the petitioners pleaded that the charges against them under the IPC be dropped and therefore the charges against them under the IT Act be investigated and pursued. It had been further argued that if the Supreme Court's ruling in *Sharat Babu Digumarti* were to be followed, the petitioners could only be charged under the IT Act and not under the IPC, for offences rising out of the same actions. The Bombay High Court upheld the contentions of the petitioners and ruled that the charges against them under the IPC be dropped". [5]

"What are the charges which will be imposed against Data Thieves?"

Because of the absence of a different enactment to deal with cyber- crimes like data theft, the charges against the hoodlum are built on the statement of the person affected. Accordingly, it is imperative that the victim knows about the fundamental laws which identify with data misuse. The act is frequently reported and punished under the umbrella of different laws.

Cyber-crime is one among the chief significant issues looked by the nations over the world recently. It incorporates unapproved access of data and break security like privacy, passwords, and so forth of an individual with the utilisation of web. cyber theft is one of the pieces of cyber-crime which implies that theft directed by methods through PCs or the Web.

The most widely recognized classes of cyber theft incorporates taking of information or personal data by means for utilizing different strategies like Hacking,vishing, email spoofing, phishing, virus attack, carding, ransomware attacks and so on with the aim of:

a) Identity theft
   - Wrongful collection of personal identity of a person,
   - Wrongful utilization of such data with a goal of making legitimate damage to such an individual.

b) Password theft, theft of data, internet time thefts etc.

c) Intellectual Property Theft

d) Internet Time theft

The most significant provisions for this regard are as contained in the IPC, 1860 (IPC), the IT Act, 2000 (IT Act) and The Copyright Act, 1957, that can be conjured against the culprit are recorded underneath:

1. **"Criminal breach of Trust (Sec 405 & 408 of IPC)" :**

"Whoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or wilfully suffers any other person so to do, commits 'criminal breach of trust' "

"Penalty: Imprisonment of up to 3 years, or fine, or both. If committed by an employee (servant), it attracts imprisonment of up to 7 years, or fine, or both."[6]

[5] Gagan Harsh Sharma v. The State of Maharashtra, 2018 BHC 1653

[6] The Indian Penal Code, 1860 // sec: 405, 408, 409

2. **"Criminal Breach of trust by public servant, or by banker, merchant, or agent (Sec 409 of IPC)" :**

"any person who is in any manner entrusted with property, or with any dominion over property in his capacity as a public servant or in the way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of trust in respect of that property, shall be punished with imprisonment for life or with imprisonment of either description for a term which may extend to 10 (ten) years, and shall also be liable to a fine."

Penalty: imprisonment for life or with imprisonment of either description for a term which may extend to 10 years, and shall also be liable to a fine."

3. **"Penalty and compensation for damage to computer, computer system (Sec 43 of IT Act)" :**

"If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network -

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;"

"(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (i) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."

Penalty: Compensatory penalty of up to Rs. 1 Crore.

4. **"Compensation for failure to protect (Sec 43A of IT Act)" :**

"whenever a corporate body possesses or deals with any sensitive personal data or information, and is negligent in maintaining a reasonable security to protect such data or information, which thereby causes wrongful loss or wrongful gain to any person, then such body corporate shall be liable to pay damages to the person(s) so affected."

5. **"Computer Related Offences (Sec 66 of IT Act)" :**

"if any person, dishonestly, of fraudulently, does any act referred to in Sec 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both."

Penalty: Imprisonment of up to 3 years, or fine up to Rs. 5 Lakh, or both.

6. **"Penalty for breach of confidentiality and privacy (Sec 72 of IT Act)" :**

"if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

7. **"Punishment for disclosure of information in breach of lawful contract (Sec 72A of IT Act)" :**

"any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both."[7]

8. **"Infringement of Copyright (Sec 2(o) and 63 of the Copyright Act)" :**

"literary work" "includes computer programmes, tables and compilations including computer data bases"

Penalty: Monetary fine commensurate with the magnitude of the offense. Further, infringement of copyright is a criminal offence."[8]

The biggest issue with regard to Data Theft arises when cross border territories are involved involving multiple countries, for example a system may be accessed in Singapore, data manipulated in USA and results felt in India. The result of such an issue is that jurisdictions, rules and laws will become an integral factor which again is an alternate issue in itself.

Couple of challenges that generally arise in such situations

- Collection of evidences in such circumstances is again a separate issue since examination in three distinct nations, who may not be in talking terms to each other makes it incomprehensible alongside the absence of specialized expertise of our cops add to the demerits;
- Lack of coordination amongst different investigation offices.
- Lack of explicit laws in the nation dealing in such crimes. Because of this, regardless of whether the guilty party gets captured, he can without much of a stretch escape by finding different loopholes in our law.

[7] The IT Act, 2000 // sec: 43, 43A, 66, 72, 72A

[8] The Copyright Act, 1957 // sec: 2(o), 63

"Does India have sufficient Laws for Data Theft?"

Indian data security laws are behind the universal bend. Despite the fact that the issue of Data Theft which is currently one of the major cyber-crime worldwide has pulled in a little attention of legislators in India, however not like the USA (US Privacy Act, 1974), UK (The Data Protection Act, 1984) and Singapore (Personal Data Protection Act, 2012), there is no particular enactment in India which can handle this issue. Be that as it may, India has The IT Act, 2000 to move toward the danger of cyber-crimes, including data theft. However, in all actuality our IT Act, 2000 isn't far reaching enough to handle the minute technological complexities engaged with such a crime.

Though various amendments have been made under the IPC to deal with cyber-crimes but still no such provision has been made which specifically covers cyber data theft. It can in this manner be presumed that the greatest cyber-crime "Data Theft" is out of the extent of criminal law in India and the IPC ought to be reasonably altered (to cover the entirety of the cyber-crimes, including data theft) at the most possible convenience of the law-making body.

The good news is that a New Legislation w.r.t. Personal Data Protection Bill has been proposed now, with the intention to ensure that any data agency/company collecting personal data of an individual will hold such data with utmost care and will only use such data for the purpose for which it is collected. Such agency/company has a fiduciary liability in case of any breach trust on this ground.

The bill clearly defines the Penalties that such agency is liable to along with the Compensation that the customer is entitled to in case such breach of trust happens. Relevant extracts from the bill is stated as below:

"Sec 57 of the Personal Data Protection Bill, 2019: Penalties and compensation" :

"(1) Where the data fiduciary contravenes any of the following provisions;

a) obligation to take prompt and appropriate action in response to a data security breach under Sec 25;
b) failure to register with the Authority under sub-Sec (2) of Sec 26,
c) obligation to undertake a data protection impact assessment by a significant data fiduciary under Sec 27;
d) obligation to conduct a data audit by a significant data fiduciary under Sec 29;
e) appointment of a data protection officer by a significant data fiduciary under Sec 30,

it shall be liable to a penalty which may extend to five crore rupees or two per cent. of its total worldwide turnover of the preceding financial year, whichever is higher;

(2) Where a data fiduciary contravenes any of the following provisions;

a. processing of personal data in violation of the provisions of Chapter II or Chapter III;
b. processing of personal data of children in violation of the provisions of Chapter IV;
c. failure to adhere to security safeguards as per Sec 24; or
d. transfer of personal data outside India in violation of the provisions of Chapter VII,

it shall be liable to a penalty which may extend to fifteen crore rupees or four per cent.

of its total worldwide turnover of the preceding financial year, whichever is higher.

Sec 2(13) defines "data fiduciary" as any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;[9]"

As we can see that this bill is definitely a need of the hour for India as it focuses on all aspects of personal data protection, however, there are still no particular provisions concerning data theft.

To Conclude

With increase in internet penetration and access to digital technology, our economy is quite vulnerable to while collar crimes including cybercrime and we're sitting on a ticking time bomb, which can be really detrimental to any individual or any corporate or the economy at large.

Though lot of initiatives have been taken to strengthen the judiciary action in the area of cyber-crime, yet at the same time there is still a great deal of inertia in enlistment and examination of cyber-crimes and hence lot of programs need to be run within the judiciary to guarantee that the people engaged with the framework comprehend the impacts of cybercrime and act quickly.

The proposed bill need to be passed on a war footing to start recognizing cybercrime as a criminal offense and hence to be judged from an angle quite different from the current definition of "Theft", using which the criminals get away easily. Laws need to be stricter and consequences need to be substantial so as to detract people from committing such crimes.

[9] Personal Data Protection Bill, 2019 : http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

References

1) Gagan Harsh Sharma v. The State of Maharashtra, 2018 BHC 1653

2) Greg Siele, *Data is the world's most valuable resource*, RingLead (April 18, 2020, 3:32 pm), https://www.ringlead.com/blog/data-is-the-worlds-most-valuable-resource/

3) Personal Data Protection Bill, 2019 : http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

4) The Copyright Act, 1957 // sec: 2(o), 63

5) The IPC 1860 // sec: 405, 408, 409

6) The IT Act, 2000 // sec: 43, 43A, 66, 72, 72A

*****