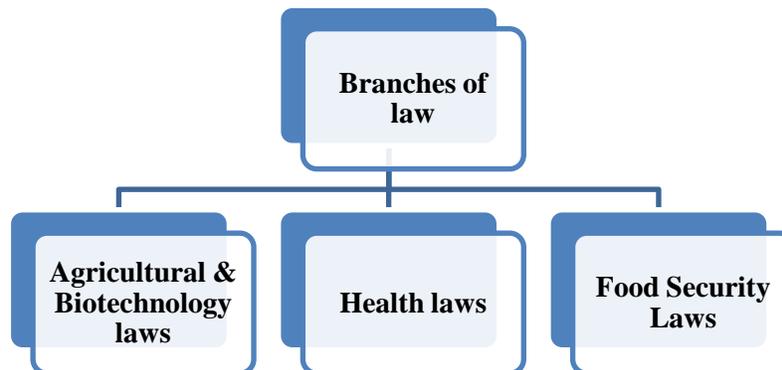


An Unreasonable Intrusion upon Person's Seclusion

MeghaSood, Harinder Biring **

Abstract

E-phase in the growing era has boosted the profitability with the stronger control in every high-tech field. Technological innovations have evinced to be a caster, which has paved the way for accorded fields of law such as:-



to flourish at the height of seven skies. Artificial governance with the technological assistance has known to be an intelligence hub, containing large number of resources to embrace every digital disruption head on. This paper will glare upon how this vaunt web has haltingly reached at the verge of selvage leading to the emanation of Data Privacy in cyberspace along with the National Security of the Nation. This paper will reflect the paradigms which are the glared matters of the daily headlines.

This paper brings into the limelight the way, how contemporaneously the development in the legal profession has managed to ante-up a stout blow to the efficacy of Intellectual Property Laws. The fabric of technological connectivity in 21st century has broadened and enrooted self-moving, self-regulating followed by self-starting adequacy of every individual.

Growing rate of crimes has ruined the civil liberties of the dwellers of each & every vicinity. Lastly this paper reveals such the risk which is always coupled with digitalization being at the crux of such advancements are impeding the credibility of the nation, once the plausibility is destroyed the society will becomes vulnerable to the crimes impeding the suave liberty of the individual in the society. So to curb the bolt of such inter connectivity an embankment comprising of legal framework is required to be used as security tool which sequentially safeguards the rights & interests of the clan at large.

Keywords: Artificial Intelligence Governance, legal development, civil liberties & Automation & Information security.

INTRODUCTION

“If someone steals your password, you can change it, but if someone steals your thumbprint you can’t get a new thumb¹”

Gordon Hunter has described that failure modes are very different. In digital era, privacy must be a priority. Appraising the same, New York, 9 October, 17:- Researchers of Buffalo University have created a computer authentication system that uses an individual’s heart shape & size to sign in, by utilizing the low-level Doppler radar to continuously scan the heart dimensions and granting access as long as the user is in right place.

PRIVACY, TECHNOLOGY & NATIONAL SECURITY

PRIVACY has been derived from Latin word “Privatus” which means separate from rest. It’s the individuals proficiency of group secludes them or information about themselves & thereby reveals themselves selectively. Thereupon one can aspire to have security by keeping privacy out of the doors but can’t have privacy without security. It is one of the basic amenity of every human being, rather than individuals alone interest with several dimensions & one of those dimension is privacy of personal data known as Data Privacy. Personal data generally refers to the information or the data which relates to a person who can be identified from that piece of lore

¹ Gordon Hunter, *Technological Advancements in the Developed Nations*, (Information Science Reference, 1st ed. 2009).

or data whether collected by any government or any private organization or an agency. CYBER SECURITY is a complex and complicated branch to manage & the acquaintance in a densely populated country like India & worldwide is not up to the mark. CYBERSPACE is such a term which hasn't carved its roots since the time immemorial. It's associated with application of internet worldwide. Consequently Cyberspace is "the total interconnectedness of human beings through computers & telecommunications without regard to physical geography". According to Warren, the object of the technological advancement is to protect the "in-volatile personality."

TYPES OF CRIMES HAMPERING THE PRIVACY OF AN INDIVIDUAL

Cybercrime encompasses a plethora of illegal activities ranging from simple hacking to cyber terrorism. Cyberspace is perpetually evolving and businesses are eager to adopt new technologies to keep up with the current standard trends. These developments create innumerable opportunities. The companies who seek to take advantage by accessing information illegally have a potential to create value and undermine their competitors. Following are some of the types of crimes²:-

1) Hacking:-

It's an illegal intrusion into a computer system, another equivalent term is cracking, but Indian Legal System doesn't support this conceptual term.

2) Cyber Stalking:-

Followed to this the internet is used for e-mails and other electronic devices to stalk another person. This term can be defined as the repeated acts of the harassment or threatening behavior of the cyber-criminal towards the victim by using internet services.

3) Denial of Services:-

This technology is driven by the influencer, which floods the bandwidth the user's mails with spam mails depriving the user, access to the Internet and the services provided there from.

4) Malware:-

It's the software which is framed to do such acts which against the law of the land with the assistance of the computer networks. It's a dissemination of malicious software with an undesirable content. Such a content can be segregated into how it get executed, how they spread or what they do.

5) Phishing Scam:-

Phishers ambushes users to a phony website, usually by sending them an authentic appearing e-mail.

Copyright infringement issues in the cyberspace could be direct, Indirect or joint.

THE REASONS WHICH BAFFLES THE PRIVACY IN RECENT YEARS

Following are some of the reasons for the growth of data privacy in India:-

²Dhawesh Ahuja, *Cybercrimes and the Related Laws* 66, (Universal Law Publications, 1st ed. 2016).

- 1) Globalization of the internet has given the acceptance to the technology in the whole world.
- 2) Easy accessibility of any information related to anyone from anywhere at any time.
- 3) The issue of enormity among the internet users giving rise to the complexities involving tracing copyright infringement to the culprit.
- 4) Adequacy to keep the information confidential.
- 5) Lack of investments & less consumption of time.
- 6) Many companies fail to find the accurate way & are most of the times unaware of the attacks.

TECHNOLOGICAL & LEGAL DEVELOPMENT IN INDIA

Internet has been the major source of announcing information, through various modes such as registration pages survey forms order forms & online contests that are not obvious to online consumers. There are chances of website owners following the consumers through cookies, tracking software etc. The right of privacy is analyzed with respect to the rights of the private parties and the constitutional rights of the state. The constitution of India doesn't deliberately grant the fundamental right to privacy. It's the courts, which have read the right to privacy into the other existing fundamental rights, i.e. freedom of speech and expression under article 19(1)(g) & the right to life and personal liberty under Article 21. These fundamental rights are subjected to the reasonable restrictions under Article 19(2) of the Constitution that may be imposed by the state.

Today the business is customer centric & the success of any business purely depends upon its users & the consumer's personal preferences, in temptation to have technological adaptations. Knowingly or unknowingly from creating a mail account to open a online banking account, all the personal information falls within the ambit of this vaunt web everywhere in day to day life. Ideally the so provided information is used with limited purpose for which it is collected but further it is to processed, transmitted and exploited for unauthorized purposes without the permission of the data owner. Lamentably cyberspace is the area where privacy and data protection are absolutely missing in India antagonistically there are "Fully Functional E-Surveillance Projects" that are actively violating the privacy rights of Indian citizens. One of the main example is that India has launched Project called "ADHAR" which straightway aspiring the demand of the circumstances to link your mobile phones, even your "PAN CARDS" emerging with the great concern of the private rights of every individual & most importantly it's not governed by any legal framework and is even not under the parliamentary security³.

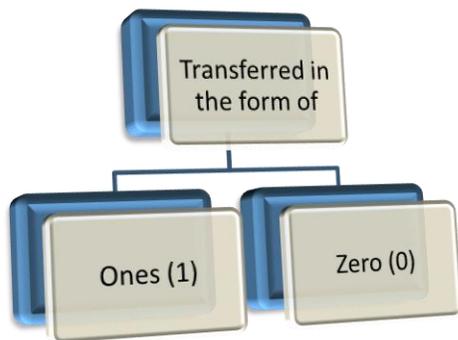
India must not only enact dedicated Privacy and Data Protection laws but it must also formulate E-Surveillance Policy of India and Indian Encryption Policy. As on date the Privacy & Data Protection Aspects in Indian Cyberspace are in really bad shape, following are the major loopholes in the present legal system:-

³Praveen Dayal '*Privacy and Data Privacy Aspects In Indian Cyberspace*, 284-89, (Universal Law Publishing Co.1st ed.2016).

- 1) No comprehensive law & still the privacy issue is dealt with some proxy has no convergence on the privacy issue.
- 2) No classification of information as public, private, sensitive information.

TECHNOLOGY & CIVIL LIBERTIES

The meaning of technology can be best explained through the case of American Civil Liberties Union v. Reno, in which it was held that “Technology is not a physical or tangible entity, but rather giant networks which inter connects numerable smaller group of linked computer networks,”⁴ But the downside of the opportunities so provided by the artificial intelligence has the unanticipated risks attaches to them. Information through computers is:-



Cyber-crimes mainly involve a computer and a network, it broadly covers the two aspects:-

1. Firstly the computer could be used to commit the crime or,
2. To be the target of ones.

Under the shade of ACLU, of Northern California has made every possible endeavor to safeguard the civil liberties in the digital era. Both technology⁵& civil liberties grow hand in hand, as the technology advances, the American Civil Liberty Union has ensured the complete protection of the privacy of the individual along with the freedom of speech and expression is also left behind.

This Union focuses on pushing back the digital censorship and government surveillance.

HEALTH LAW

Health law in general parlance is an interdisciplinary field which is inclusive of any law affecting the health of the individuals & the public at large. This field of law is comprised of such specific laws Some of the focused areas in the health laws are:-

⁴ Dr. Srinivasulu, *An Overview of Privacy, Data Protection and Cyber Security in India*, 67 (Interstice, 1st ed. 2014).

⁵ Agnes Flavia, *The Technology & Innovation*, 37 *JILI* 125 (2001).



To strengthen this field, government is taking initiative, for the better upliftment of the upcoming of the law in the field of health.

This field of law is particularly concerned with the health of the individuals & population. So therefore it has become an obligation for each nation to provide the best healthcare services & its timely operation.

Following are the instances of the health laws which are inclusive of:-

1. Advancement of the healthcare policies such as Universal Health⁶ coverage.
2. Establishment of the basis for the organizations and financing of the country's healthcare systems.
3. Preservation & protection of the public & social nature of healthcare.
4. Controlling the training & practice standards of health care.
5. Followed by addressing non-communicable diseases risk factors such as smoking.
6. Last but not the least, to regulate the collections & suitable use of the health related information.

ARTIFICIAL INTELLIGENCE

Artificial intelligence is changing the cyber security but has unfortunately failed to catch up all the solutions for the cybercrimes so committed by the hi-tech learned criminals.⁷

AI is often confused with the automation, but in reality both are two separate methods to solve the common problems.

Undoubtedly automation has entirely given the new ways to operate the business. Beginning from the factory to the back-end of the It, automation has tremendously increased the speed of productivity likewise freeing the every worker of the IT group, to focus particularly on more skilled tasks, thereby raising the economy of the nation as a whole.

The system of Artificial Intelligence is constantly in the state of change. Meaning thereby the AI is a great fit for cyber security, where every malicious actor is continuously developing new attacks. Organizations are now-a-days facing everything from ransom ware to stealthy "unknown unknowns" that has bypassed the traditional perimeter defences to silently carry out the espionage over the long period of times.

⁶Clayton Christensen, *The Innovator's Dilemma*, 205-06 (Harper Business Reprint ed. 2011).

⁷Kevin Kelly, "The Inevitable," *The Economic Times*, Jan. 07, 2019.

There are times when these hi-tech organizations even often make the use of traditional methods to deal with their own massive volumes of the vulnerability to compound up with the problems on a whole. In the words of Andrew Tsonchev, “that there is no silver bullet for cyber-security on a whole.”⁸Cyber-security market is flourishing at an alarming rate, it’s the machine learning industry buzzwords, but many innovations are there which still require rules & signatures of previous attackers.

ARTIFICIAL INTELLIGENCE GOVERNANCE

So due to the growing rate of cybercrimes & flowing of the power into the hands of malicious criminals the time has come to make the use of Artificial Intelligence in the governance as well. In the past year of 2018, there are reports of happening of such devastating events, which has ultimately left the population spellbound & has shaken the roots of democratic nation like India, Studies of Aug.19, 2018, 13 coaches of the passenger train were derailed thereby killing the 24 people & leaving 200 & more people in pain & injury. Followed by this event on Sept.29 of 2018 itself 23 people had died due to stampede on the pedestrian of the foot-bridge in Mumbai, seeing such crushing & helplessness events are the everyday paradigms of the daily newspapers. But on a whole AI has proved in the modern era has given us the means to make the leverage of every minute part of AI to manage the operations of the ailing company, to efficiently detect the frauds, in a better manner.

So by governing the entities of the modern era whereby AI doesn’t necessarily gives the productive approach for the governance of the business on a whole.

AI is just the mode to get the things better, faster, cheaper & last but not the least gets it in more accurate manner.

AGRICULTURE BIOTECHNOLOGY AND FOOD SECURITY LAWS

Security as to food is one of the basic amenity for the survival of the mankind. In the developed Nations food security can be substantially improved by increasing the investments & policy reforms simultaneously.⁹While on the other hand Agriculture & Biotechnology has ability to eliminate, malnutrition & hunger through the production of the ample of crops which would be resistant from any kind of pests & diseases & thereby having:-

1. Longer shelf-lives,
2. Refined textures & flavours,
3. High yields per units for land & time,
4. Weather resistant & tolerance of all kinds of soil conditions,
5. Generating employment at the grater scale,

Thereby not over-emphasizing on the one point but also maintaining the equilibrium of every caster of both resource & the product on a whole. The advanced technology can be applied to

⁸Jef Akst, *Exploring Life Inspiring Innovation*, 97 (Printice Hall India Learning Private Limited, 2nd ed. 2018).

⁹D.Majumdar, “*The Role of Agricultural & Food Laws in shaping the economy of the Nation*,” *The Economic Times*, 9 July 11, 2017.

improve the agricultural production so as to improve the food production for the human population in an environmentally suitable manner. However, there is a great need to have a collaboration of both government & private bodies to invest in agricultural biotechnology based companies, researches & initiatives in order to make the gene revolution beneficial for the developing countries.

THE FUTURE OF LAW

Technology has so far occupied an important milestone & India's democracy keeps its eyes on the fundamental right to privacy particularly in the phase of technological advancement while treating its every citizen in accordance with laws. It settles a debate that arose from the legal challenges to Aadhaar program which undoubtedly infringes upon individual privacy by recording biometric details & since it is must for a number of other obligations such as filing of income tax return. Technology undoubtedly shields the individual from non- government entities¹⁰. One of the top social priority of every data is WhatsApp, but today it not only singles out technology for being a challenge to privacy, but also recognizes that an understanding between two people can't be the basis for a third person to infringe upon someone's privacy. Technology has made it possible in modern era to enter into citizen's house without knocking at the door; this is equally possible both by the state & non-state actors. It's solely the individuals choice as to enter his house, how he lives & in what relationship.

Technology includes electrical surveillance which involves monitoring the people often without their knowledge. Technology influences the processing of both personal & private information of an individual. Technology is now-a-days used as a value laden process; it has ontologically changes the status of a document with accompanying ethical implications. The interception & reading of email messages, this poses an ethical problem which relates to a private communication of the individual. The main problems include the fact that the individual are not aware of personal information being integrated into a central, that the individual doesn't know the purpose for which the integration is affected. Every action takes the leaves trial information that could be recorded & stored for the future use. The move from one set of dominant information technologies to another is always morally continues. In a diverse country like India rich in data & the technology to record store vast amounts of this data has grown rapidly.

The primary moral concern is that to collect, store, access information is done in a just manner that anyone can see is fair & is the best interest of all parties involved.

CONCLUSION

Privacy & Data Protection are the two core requirements for the effective functioning of the civilized nation. Be it any organization or the individual, everyone preserves the right to protect the personal, sensitive & commercial data as well as information. There is no dedicated data privacy & data protection laws in India. Internet has paved the pace of the functioning of every sector in the modern scenario & is a rapidly spreading phenomenon in the world. Technological

¹⁰Allec Ross, *The Industries of Future*, 49-55 (Simon & Schuster, 1st ed. 2013).

advancements have always been bait for increasing criminal applications & the internet is no exception. Many new possibilities have opened up for the perpetration of crime. The illusion so created by this dark web of virtual world to the information seekers has incepted all over the world. The three organs combined efforts have been tackling the problems by introduction various laws. Definitive steps have been undertaken by the government of India so that it lives up to the objective of improving the transactions online & facilitating the plans of Digital India campaign so launched in India. So in the light of above, there is a dire need of plugging the loopholes in the best interest of the country.