LEGALFOXES LAW TIMES

INNOVATION IN INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

By Aanya Agarwal and Dhruv Singh

KEYWORDS- Technological advancements; Innovation; IT Act, 2000; Cybersecurity

ABSTRACT

The way technological development is taking up the pace, isn't it ludicrous that we stick to the same old law that was in force before these advancements? Every corner of the world is making a discovery, and it is not only making us more developed but also more vulnerable to the new dangers of those discoveries. Therefore, keeping this thought in our mind, this article is written to provide insight into some innovative technologies and the legal standpoints related to them.

INTRODUCTION

"*Any sufficiently advanced technology is indistinguishable from magic".*

– Sir Arthur C. Clarke

Technological advancements have seen meteoric inflation in the last few years with an extraordinary effect on the general public. In today's era, technology has transformed our way of living in the manner of how we walk, play, or interact with others. With the extensive use of mobile phones and cellular data, individuals have connected with their peers, family members, and colleagues through e-networking websites, video call applications, and e-mail platforms. Further, because of these technological abilities, vast new businesses and industries have taken to electronic commerce. One need not visit the workplace, supermarket, or shopping complex to

purchase the various commodities and goods. Not only this, perhaps anyone sitting at home can experience real-life activities by sitting on their couch through Virtual Reality (VR) or Artificial Intelligence (AI). Some of the other advancements, such as blockchain and cryptocurrency in the field of technology, have been discussed in this paper. In hindsight, it is a grievous matter at hand. As the years have yielded headways in the different innovative fields, so have the wrongdoings expanded. Thus, today because of high web infiltration and cybercrime, cybersecurity is one of the greatest "needs" of the world as cybersecurity dangers are exceptionally hazardous to our nation's security.

Blockchain

From securing online transactions to making them quick and efficient, blockchain has gained attention all around the globe. Blockchain is a network of computers which enables peer-to-peer transaction without the need for an intermediary body. Each transaction is validated along with a group of validated transactions that is called a block. It is further added to a chain of blocks, coming to be known as a blockchain. The information present in such blocks cannot be altered once added to the chain, which is the key to its impregnable security.

Apart from having some considerable benefits from using blockchain-like increased efficiency, permanent and immutable transaction records, some shortcomings can attract legal attention, like blockchain provides anonymity which makes it a tool for money laundering and terrorist funding, these circumstances can attract criminal securities fraud laws. Also, it is subject to cybersecurity risk from hackers for instance if an entity successfully acquires more than 51% of network nodes then he can control the whole network which is one of the major problems of the blockchain network.

Countries like the USA have agencies to stop these fraudulent activities, one of them is Securities and Exchange Commission (SEC) which has specified the issuers to register the coins or token and it must constitute a security. These regulations will put a stop to investors getting involved in fraudulent activities.

Cryptocurrency: Reliable or Not?

Cryptocurrency is just a smaller version of virtual currency. The difference is in the technique used for transactions. A technique named cryptography is used for encryption and decryption of cryptocurrency that makes it more efficient and secure. Having no physical existence, their ownership is through entries in the blockchain. Its value largely depends upon the demand of users, as opposed to virtual currencies that can be legal tenders. Cryptocurrencies are still not recognized as legal tenders anywhere i.e., they cannot replace paper based-currency. Consequently, they require agreement by the users for a successful transaction.

Some cryptocurrencies are now associated with NASDAQ (National Association of Securities Dealers Automated Quotations) which is an American exchange. This step surely helps in addition to the legitimacy of cryptocurrencies. Although the way to NASDAQ is difficult, several cryptocurrency exchanges worldwide have made it possible.
Some examples of cryptocurrency are Bitcoin, Ethereum, and Ripple.

Artificial Intelligence: A Way Towards Future

AI or Artificial Intelligence means a computer system working on algorithms that not only gives the output for the given input but also finds a pattern in those inputs and can learn from past experiences to respond to different outputs on its own.
Although this technology is a game-changer, in addition to that it has also raised questions related to a law that needs to be dealt with by countries in recent times. The fields in which AI is being used are limited, but prospects are bright hence the law also needs to be evolving to handle the situations caused by this technology to protect the innocents from being harmed.

Some legal questions that have been raised till now are:

1. Privacy: Data being used by AI raises an alarm for the users because their data can be used by the developers or any third party involved. Many regulations and guidelines are coming into force to minimise this concern like the “General Data Protection Regulation” (GDPR) enacted by the European Parliament which puts a bar on organizations to collect unauthorised data of users.

2. Liability: In the case of AI, if something goes wrong, who is to be held liable - the user, the developer, or the machine? NITI Aayog provided answers to these questions in its National Strategy on Artificial Intelligence #AIForAll that Negligence test. It should be conducted instead of Strict liability, and the parties should bear proportionate liability in place of joint and several liabilities.
3. Biased decision-making: Some countries have started using AI in court proceedings. AI is based on algorithms and it makes its decisions based on patterns. So what if the decisions are biased? It is a possibility that AI-based technology can give influential decisions because the society that we live in is biased. If such a source decision was partial in nature, so will be its individual decision. Therefore, solely depending on AI is not an option yet.
4. Breach of Contract: AI works on data. The more the data provided, the more it works efficiently. Now, what if it starts using data for another purpose on its own? A simple solution to this problem would be forming a contract between the user and developer for some fixed work for which the AI is being sold. If it does any work outside that field, the developers can then be held liable for breach of contract. Therefore, they will be more cautious while programming the algorithms.

Cybercrime and Cybersecurity

Suffering from attacks that can make you bankrupt in seconds or which can have access to all your data is a crime that arose post invention of the internet, having altogether different dimensions. Such crime was later acknowledged. Moreover, due to the continuous evolution of various technologies, the law is still evolving and hasn't covered all corners of these numerous crimes. Cybercrime means any crime which is related to Computers and Networks. For example, carrying out extortion, abusing security utilise computerised information from Computer frameworks and other electronic devices.

Cybersecurity proposes ensuring the safety of information, systems, programs, and other data from unapproved or unattended access, devastation, or change. Cybersecurity is significant because it assists by making sure about data and our framework from infection assault.

India has enacted the I.T.Act, 2000 based on the UNCITRAL (United Nations Commission on International Trade Law) model recommended by the general assembly of the United Nations by a resolution dated 30th January 1997. Chapter XI of this Act deals with offences/crimes alongside several other provisions scattered in this Act.

A few major cyber attacks are discussed in this section -

Nigerian Letter Scam or "419" Fraud- This fraud attracted attention around the whole world. In the scam, a self-proclaimed government official offers an opportunity to an individual to earn some illegal money by providing their personal financial information. This whole trap was set up to drain the bank account of the individual. Consequently, millions of dollars were stolen through this scheme.

WannaCry Ransomware Attack- The WannaCry ransomware attack was a worldwide cyberattack that took place in May 2017 by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through EternalBlue, an exploit developed by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called 'The Shadow Brokers' at least a year before the attack. While Microsoft had released bits earlier to close the exploit, much of WannaCry's range was from organizations that had not applied these or were using older Windows systems that were past their end-of-life. These patches are imperative to an organisation's cyber-security. Yet, many were not applied because of needing 24/7 operation, risking having applications that used to work break or other reasons.

Furthermore, discovering new angles and using them as an attack by cyber hackers cannot be stopped entirely. The regulations and amendments, on the other hand, can be made regularly to deliver justice.

CONCLUSION

"*It has become appallingly obvious that our technology has exceeded our humanity".*

– Albert Einstein

Advancement in technology is not only a mere requirement but a necessity to make sure that an organisation or country stands a chance in this cut-throat competition. As it is rightly said by William Blackstone, "all presumptive evidence of felony should be admitted cautiously, for the law holds that it is better that ten guilty persons escape than that one innocent suffer". Therefore it becomes a duty to protect them from such evolving yet unfair world and this responsibility lies on the protrusions of law.

Though one cannot expect regulations to be brought into effect before the practice of such acts, they must be enacted at the earliest. Furthermore, it is pertinent to take into consideration that some countries still do not accept the use of such technologies, and not only does it make them debilitated in a competitive market but also makes them vulnerable to unfair and illegal activities.

Therefore we can say that it is largely unknown how the law will deal with these technological advancements but adopting new regulations like IT Act, 2000, and amending them from time to time is the first step towards legal development.