Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2021 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Importance of Data Protection

S Ashwath[a]

[a]Bennett University, Greater Noida, India

Received 12 June 2021; *Accepted* 25 June 2021; *Published* 28 June 2021

One of the most disruptive crimes for financial markets but very versatile that it can spread to other forms of crimes as well. Cyber-crime is one of the most Underestimated crimes in the world right now. It is already a big problem, and it is not stopping. It's growing so fast that law enforcement is scrambling to catch up. It can be left to the police to take care of this, but it is clear some things are meant to be handled by the right bodies and in this case, it is the law. It is said that as time goes cyber-crime will outnumber traditional crimes. This paper shows the importance of data protection and creates awareness of how even the powerhouse countries are suffering, and it is not a joke if UK and US and falling victims to this. It is very important to gear up for this upcoming threat that can only be solved with the world coming together and sharing their knowledge and expertise in different areas which will create a powerful team to stop this.

Keywords: *data, protection, hacking.*

INTRODUCTION

The first ever cybercrime happened in 1834 where a couple of robbers hacked the French telegraph to steal information related to stocks[1]. Although there are some sources which state

[1] Sauvik Acharjee, 'The History of Cybercrime: A Comprehensive Guide'(*Jigsaw academy*, 13 February 2021)<https://www.jigsawacademy.com/blogs/cyber-security/history-of-cybercrime/> accessed 02 June 2021

that 1820[2] was when the first cyber-crime occurred. That was because at that time the first computer was also there at that time. The incident was where the then said computer Abacus, was hacked. Even though there is the confusion it can be said that during the 1800s the first cyber-crime was committed. Even though the first cybercrime was recognized in 1834, the first cyber-criminal was recognized in 1981[3]. His name was Ian murphy who hacked the AT&T network and changed the internal clock to charge off-hours rates at peak times. This was the first-time cybercrime was born into the world. After that, there were plenty of crimes related to the internet, but it all boomed during the 2000s when everything started getting digitalized like social media came up. This led to a lot of personal information getting stolen. At this point, cyber-crimes have evolved so much that they are no longer phone phishing cases but much more which is very hard to comprehend Right now the most concerning one of them is the compromising of personal data. Stealing of personal data is leading to a lot of problems in the present world. Seeing this it can be said that cyber-crime is no simple issue. Cyber-crime is not yet a recognized and a formulated law in the world. It is still evolving as the day goes forward. This is what this article will help go through thoroughly with the help of other countries like the U.S, the U.K and so on which are facing crimes like this or formulating laws to stop this.

DEFINING CYBER CRIME

Till date other than mentioning cyber-crime or cyber terrorism in law there is no proper definition for it. So, what is cyber-crime? It is basically any criminal activity that involves the use of a computer or a network or a network device. Most of the cyber-crimes that occur are carried out to gain profits illegally. But there is still the other side which targets the computers and disables them. This happens through scams and other mediums where the virus is generated onto the computer and later spread to the whole network. Sometimes both of those occur at the same time. while the network is getting corrupted any chance of profits would be

[2] Arshi Khan, 'The First Recorded Cyber Crime Took Place in the Year 1820' (*Scribd.com*) <https://www.scribd.com/doc/71120466/The-First-Recorded-Cyber-Crime-Took-Place-in-the-Year-1820> accessed 02 June 2021

[3] Vuk Mujović, 'Where Does Cybercrime Come From? The Origin & Evolution Of Cybercrime' (*LE VPN*, 18 October 2018) <https://www.le-vpn.com/history-cyber-crime-origin-evolution/> accessed 02 June 2021

taken away. Finance is the primary target for cyber-crimes. Ransomware assaults, email and internet fraud, and identity fraud, as well as attempts to steal financial accounts, credit cards, or other payment card information, are all examples of profit-driven criminal activities. The department of the U.S has divided the crimes namely computer being a target, for example, to gain access to network access next is the computer used as a weapon like to launch a DoS attack and lastly, the computer used to aid the crime like the computer is used to store illegal data. The European convention on cyber-crime where the U.S is a signatory had defined Cyber-crime[4] as a broad variety of hostile behaviours, such as illicit data interception, system interferences that jeopardize network integrity and availability, and copyright infringements. Normally cyber-crimes are carried out by a single person or a group with little to no technical skill or on the other hand there are also highly skilled technicians who as a group organize global crimes related to the internet. They are normally targeted at the countries with weak cyber laws or countries with non-existent cyber laws. Cybercriminals utilise a variety of attack vectors to carry out their cyberattacks, and they are always looking for new ways to achieve their objectives while evading detection and prosecution. Getting an idea of this, the next topic to gain access would be the most famous crime of U.S, U.K, and India. Analysing all of that would help decide which law system would work for India.

UNITED STATES OF AMERICA

There are a lot of major and famous cyber-crimes but for this article one of the most infamous and scandalous crimes shall be taken. This incident was also infamously called the Facebook and Cambridge Analytica incident. The name says it a lot but nonetheless, this happened in the year 2016. What is Cambridge Analytica[5]? It is a data analytical firm that worked with trump for the 2016 elections. So, using that as an advantage basically, the company gathered the details of every citizen in the United States and started advertising which is known as psychographic advertising. Psychographic targeting. Psychographic Targeting or psychographic segmentation is basically where a body explain and forecast people's

[4] Kate Brush, 'cybercrime' (*Techtarget.com*) <https://searchsecurity.techtarget.com/definition/cybercrime> accessed 03 June 2021

[5] 'The Cambridge Analytica Story, Explained. A quick, but thorough, overview of the controversy.' (*Wired*) <https://www.wired.com/amp-stories/cambridge-analytica-explainer/> accessed 03 June 2021

behaviour, splits people into subgroups based on shared psychological features, such as subconscious or conscious beliefs, motives, and priorities. So, in this case, since Cambridge Analytica was working for Trump, they targeted an audience that did not support the Republicans. How did they do that? Their company uses various means to gain data but, in this case, they gained it via a third-party app 'Thisisyourdigitallife' which was developed by the students in the University of Cambridge's psychometric centre[6]. This not only allowed the company to acquire the data of the people who downloaded it but also their friends and so on. That is why it is important to read the terms and conditions of every app. But even though they got it, how did they use it. As told before about the psychographic targeting, they started feeding ads related to trump in a positive way for citizens who did not support the republicans. Not stopping there, they also posted feeds praising trump to the republican supporters as well because their aim was to gain supporters and on the same side hold the people who support the republicans as well. But how was this directly connected to trump? That is solely because for the 2016 elections Trump decided to do digital campaigning which focused on ad targeting. Hence, the accusation. So, in this whole scenario, where does Facebook come from? After acquiring data through the third-party app using fakebook's open ended data of the people started posting ads in their feeds. So, the accusation was on how they firstly derived data illegally from Facebook (or if Facebook was also in this plan) and how Facebook (if the data was stolen) manage to get it stolen because they had promised to keep their data safe. In simple words, the problem is, how did Cambridge Analytica manage to get the data of approximately 50 million Facebook users without their permission and how was Facebook careless enough to let it out so easily. Facebook faced a huge blow because it is one of the top social media platforms and holding more than a billion users' personal data is not a small thing. At first, when the investigation was going on they could not prove any of the accusations thrown at the company. Later when the whistle-blowers came out and spread what was going on it made it easier. But did it serve full justice? No. This shows how strong the plan was and how sure they made themselves to execute it without any problems. One company changed the whole outcome of the elections and changed the way the country will

[6] *Ibid*

move forward for the next 4 years. Seeing all this the idea is still not clear as to how the company got the data of the citizens. Some say the data was sold by a Facebook employee to the CA. some say it was hacked but no matter what the reason is, the citizens were hacked. A hack so huge that instilled in people's fears. The founder and the CEO of Facebook were called and scrutinized for the careless move that was done by the company and later as per them the mistake was done by one of the employees and he was fired from the company. Later Mark sent a letter apologizing for his mistakes. On the other hand, the CEO of Cambridge Analytica was fired immediately. As for the company, it is still a mystery. Thus, coming this far it is a crime of compromising the data of people and the data protection is a huge stake here and the world moving at this rate, not having any privacy of the data is not a small issue. This shows how dangerous the internet can be and how badly this world needs data protection laws and much more.

UNITED KINGDOM

This country's most famous cyber attack would be the WannaCry ransom attack[7]. This attack had affected more than 200 countries, but the UK had faced more damage than expected. So basically, it was a ransomware attack in the year 2017. It focused its attack on computers running the windows os which was outdated like the windows XP or windows 2003 and so on. The attack also made it with the help of encryption unable to load or access the data. It was also considered to be a worm that can spread to other computers with the help of the network. The first victim of the attack had given a notice stating that 300$ will be paid if they take off the virus. The damage caused by this attack cost billions of dollars. Till date, no hacker has owned the attack but with a good effort of investigation, it was traced back to North Korea and hence the assumption that it is from there. The WannaCry had exploited the vulnerability which was present in the Windows implementation of server message block protocol. Based upon some sources it is said that this same problem is present in the NSA as well (US National Security Agency). But the difference between both is that WannaCry used it for exploiting rather than helping or issuing this issue. Although they were not able to pinpoint the right

[7] Rami Akrem Addad and others, 'WannaCry Ransomware and its impact on the UK's National Health Service' 6 (*Ashwa*) <file:///C:/Users/ashwa/Downloads/Case_study_mosaic_team.pdf> accessed 06 June 2021

reason as to how it spread, it is said to spread by mail in the beginning. One of the problems this attack caused in the country was that the NHS (national healthcare service) was severely affected. The NHS was the largest healthcare service in the country that was first funded by the government when founded in 1948 but soon started getting support from various national insurance. It serves all the citizens and the legal citizens of the country. Between May 12th and May 19th, 2017, the NHS was the target of a WannaCry ransomware attack. Some NHS trusts have been individually targeted by cyber assaults in the past. It is not new for the NHS to get hacked but WannaCry was considered as one of the largest attacks in the history of NHS. Funnily enough, NHS had gotten a warning of cyber attacks 1 year prior to the attack stating that hacking could cause compromising of patients' data and could cause huge amounts of problems. It would be an exaggeration if it is said that they did not take any steps hearing about the warning, but it was clearly not enough to prevent the attack. As mentioned previously, Due to the extent of the damage, the WannaCry cyber-attack is regarded as the most dangerous strike the NHS has ever seen or experienced. NHS England does not know the full scope of the interruption, according to the NAO, although at least 34% of trusts have been affected. In fact, 80 out of 236 trusts in England were reportedly[8] affected, with 34 being infected (i.e., the machines were locked out and the files were encrypted) and 46 experiencing service outages. In the case of the latter, they immediately turned down their gadgets after learning of the attack to prevent the ransomware from spreading, and they carried on with their daily routines using paper. Because ransomware is used as a technique for blackmailing, it causes a lot of damage[9]. Furthermore, if the attackers can make money, they will continue to improve their attacks. The WannaCry ransomware demonstrated that such assaults could have a global impact. Furthermore, sensitive industries, such as the UK's National Health Service, may be impacted. This case proved how important it is to save the data of people.

INDIA

[8] *Ibid*

[9] *Ibid*

There are two cases for India including the recent scandal that is going on. The first one is the hacking of UIDIA also known as the Unique Identification Authority of India. According to an investigation[10], the Aadhar which was used to enroll new users or existing users to the database might have been hacked using a software patch. The software patch had the ability to disable the critical security features. This software patch was available as low as just 2500Rs. This allowed unauthorised people to enter the site and generate anybody's Aadhar details irrespective of the place. As per the investigation, this patch was able to bypass the security because at that time the private companies were also helping enroll citizens into this. But UIDIA had denied all these allegations and stated that this was all baseless and hence the hacking could not be confirmed fully. Later in an investigation conducted by the tribune showed that it was indeed available where the people could generate anybody's Aadhar details and get away with all the personal details. Even then they denied these allegations. Not stopping there even RBI probed UIDIA to release the 210 government websites that were made for Aadhar, but they denied it and stated that the time frame is still not confirmed for the leak hence details can not be given. Earlier at the time of the introduction of Aadhar, the French security researcher pointed that there are many loopholes that allow hacking of this site very easy but even up to that point UIDIA stood by their statement strongly that it is a secure and safe biometric system, and all the citizens must take care of is to not share their persona details related to that. This instance showed that they did not accept these allegations but there was still concrete proof that this had happened. The next problem that awoke recently is the new government policy[11] for social media platforms especially WhatsApp where there was a new policy that had to be signed by them. But his policy as per the Facebook owner is abridging the right to privacy. This is because before this policy had come out WhatsApp was always an encrypted-to-encrypted messaging service which means both the receivers and sender can send messages without interruption. This was what the terms and conditions said

[10] 'UIDAI Aadhaar Software Hacked Using A Patch That Disabled Critical Security: Report' (*Firstpost*, 11 September 2018) <https://www.firstpost.com/tech/news-analysis/uidai-aadhaar-software-hacked-using-a-patch-which-disabled-critical-security-report-5159521.html> accessed 08 June 2021

[11] Joseph Menn, 'WhatsApp sues Indian government over new privacy rules' (*Reuters*, 26 May 2021) <https://www.reuters.com/world/india/exclusive-whatsapp-sues-india-govt-says-new-media-rules-mean-end-privacy-sources-2021-05-26/> accessed 08 June 2021

anyways. Now as per the terms and conditions, the encryption should be removed. The governments' defence for this is that the messages were always traceable and agreeing to the policy makes it easier. But why should this even come about, this is because WhatsApp has a lot of rumours spread and the government does not want a bad image about them to be spread during the covid times unnecessarily as that could bring about problems. Are those problems true or not, This is for another article. So, what will happen if WhatsApp does not accept the terms and conditions? Normally WhatsApp is only a third-party platform so if anything, illegal or bad happens then the sender or receiver will be held responsible. This is only if WhatsApp agrees to the terms and conditions. If they do not, then WhatsApp will be the one responsible. This issue has problems on both sides. It is not unknown that Facebook is a "privacy protector". But if what they say is true then the government is also at fault because it violates one of the most important fundamental rights which is the right to privacy. In this instance, it is again shown how important data protection is and why is it needed to be protected.

NEED FOR DATA PROTECTION

Data is a very important piece of information that consists of all the personal records which are very important for every human being. Cybersecurity basically hinges on data protection. As the world moves forward data is becoming one of the most precious commodities out there and it is obvious that crimes related to this are going to intensify. As per certain reports, we create more than a trillion bytes of data with more than a billion devices interconnected with several networks[12]. It is obvious it is this is going to grow as we go forward as well. Seeing this, it is important to know that data protection is very important and hence could prove as a complicated task. There are many countries that have the legislation for cyber-crimes but there also countries that do not have a draft also. Countries like the US have Computer Fraud and Abuse Act which is the main statutory mechanism that deals with cyber-crimes. To be specific 18 U.S.C section 1030[13] deals with these crimes. In the UK[14] it is the Computer Misuse Act 1990

[12] M K Narayanan, 'The world is hardly wired for cyber resilience' *The Hindu* (India, 14 June 2021) 6

[13] Computer Fraud and Abuse Act, U S C 18 S 1030

[14] Misuse Act 1990

and in India, it is the Information Technology Act, 2000[15]. But it can also be governed under the IPC. This came about because of a case[16] that brought confusion as to which will be used. At the end of the case, it has prevailed that the IT act will only be considered. One thing must be noticed though and that is the fact that This act has only mentioned all the crimes and given punishment for it but are those punishments enough? What if there is murder through the internet will that come under the CRPC or the IT act. Questions like that are still floating around and that is still a concern. It is true there are many countries that do not have the legislation yet and it is great to have legislation at the least in India. For the present world that is not enough. Hence this paper shows how fast the world must move to improve the protection of data. Data is of two types[17]. The date at rest (Transmission through insecure networks) and data at motion (Consuming data). With the development of the cloud and mobiles, it is starting to become more common for hacking. Cloud sources are more space for personal data and if that is hacked then trust starts going down in everything. The creation of new and advanced technology is needed new technologies like Artificial Intelligence, machine learning, and so on. Just like countries that have no legislation, there are also countries that have developed their artificial intelligence and machine learning which will give them an added advantage. In India not only should the technology advance but pressure needs to be put upon public officials and company officials to carry out tests regularly to see the vulnerability and improve them. This is only the start there are so much more. But it is always better if there is a start that will help in the long run.

CONCLUSION

India is ranked no.2 among other countries for getting affected by cyber-attacks. After the development of IoT, there was a 22% rise in the crime rate[18]. This is the second time in a row they ranked this high. Reading this far it should have given a constructive idea as to how we are going to live in the future and how important it is to protect the reason for living for the

[15] Information Technology Act 2000, s 66(D)

[16] *Sharat Babu Daggubati v Government of NCT of Delhi* AIR 2017 SC 150

[17] Narayanan (n 12)

[18] Pallavi Dutta, 'Cyber Threat Report of 2019: 69% of Firms Face Serious Cyber Attacks in India!' (*Kratikal*, 1 November 2019) <https://www.kratikal.com/blog/5-biggest-cyber-attacks-in-india/> accessed 08 June 2021

future. There is an increase in the use of information technology and the internet protects these data which is very scary for every person right now. Losing that or getting hacked could result in a huge disaster and nowadays these crimes are affecting everybody on a larger scale. The internet is used to collect and spread information. If crimes are occurring in that field continuously then the law should also be there to protect it. In a world where soon, everything is going to be the technology it is very important to build trust in these matters. If nobody acts accordingly then it will cause a huge amount of chaos. That is why Protecting Data is very important. The journey of compliance has just started, and it is very important to be pro active rather than reactive for these matters. It might be appropriate to end this with a quote by the chairman of IBM, Arvind Krishna who said that cybersecurity will be the pressing issue of the decade and that value lies with the data and the people will be coming for that data.