BAOU
Education for All

स्वाध्यायः परमं तपः

Dr. Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-204 Emerging Issues of Cyberspace

Post Graduate Diploma in Cyber Law

(PGDCL)

2021

Emerging Issues of Cyber Space

Dr. Babasaheb Ambedkar Open University

Emerging Issues of Cyber Space

Course Writer

Dr Peter Ladis	Faculty of Law, Chankaya National Law University, Patna, Bihar
Dr DeeshaKhaire	Faculty of Law, Gujarat National Law University, Gandhinagar
Ms PrabhavatiBaskey	Faculty of Law, Gujarat National Law University, Gandhinagar

Content Reviewer

Mr Kumar Gurav	Faculty of Law, Chankaya National Law University, Patna, Bihar

Content Editor

Prof. (Dr.) Nilesh K. Modi	Professor & Director, School of Computer Science Dr.Babasaheb Ambedkar Open University, Ahmedabad

ISBN:

Printed and published by: Dr.Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr.Babasaheb Ambedkar Open University

PGDCL-204

Emerging Issues of Cyberspace

Block-1: Introduction to Emerging Issues under Cyber Law

Block-2: Artificial Intelligence and Cyber Law

Block-3: Data Protection And Privacy

Block-4: International Law On Digital Rights

Block-1

INTRODUCTION TO EMERGING ISSUES UNDER CYBER LAW

Unit 1: A STUDY ON EMERGING ISSUES ON CYBER LAW

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

In this chapter we will learn-

- The challenges under cyberspace and the urgent need for reformation in India's cyber edict framework and various issues in which cyber law enforcement lacks.
- Provisions governing cybercrime in India.
- Suggestive measures to deal with cyber law.

1.2INTRODUCTION

In the scenario of technological development, around the world, it is rapidly growing in a very positive way. But along with that few anti things also comes to the limelight. One of the aspects is rapid growth of digital and network technology, which helped in developing a virtual world of cyberspace. Cyber space brings great boomin every field of lifestyle and economy but parallel to the same, there is a growth of new crime, which is called cybercrime. The internet was originally designed as a medium for science and knowledge exchange, but it is now used by both the victim and the perpetrator to conduct cybercrime. Communication, ecommerce, and e-governance became more transactional as time went by. Cyber rules cover all compliance questions pertaining to internet violence. As the number of Cybercrime such as unauthorized access and hacking, Trojan attack, virus and worm attack, denial of service attacks etc. are increasing; the need for related laws and their application has also gathered great force. Cybercrime has neither the origin, nor the reference in the law.[1] On the tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to cyber space, cybercrime was divided into two categories and defined thus:

(a) Cybercrime in a narrow sense that is computer crime in which any illegal behaviour done by the means of electronic operations that targets the security of computer systems and the data processed.

(b) Cybercrime in a broader sense which is computer related crime any illegal behaviour committed by means of an operating system or network, including such

[1] ManeeshTaneja and Dr. D.B Tiwari," Cyber Law", International Referred Research Journal, vol.11 (21) October, 2010, pp. 63-65.

crimes as illegal possession or distributing information by means of a computer system or network.

According to the tactical aspect attacks to digital networks for the purpose of seizing control or even destroying infrastructures that are vital to governments and sectors are of the crucial importance. According to the Norton report frequency of cyber attacks on Indian assets, with the government and private infrastructure equally exaggerated. In July 2013 government published national cyber security policy and just after that it was reported that government official's emails had been hacked. The NCSP is far from answering all nuances of the cyber threat. It doesn't maximize its potential for optimum benefit it just only provides guidelines for the standard operating procedure. The crucial point of security concern related to telecom industry which is fully integrated into cyberspace is missing.[2]

In this a steady increase in number of such crimes in this area is expected which demands for greater attention of lawmakers.

1.3LITERATURE SURVEY

The advancement in technology has resulted in an increase in illegal activity, and the IT Act of 2000 establishes procedures for dealing with cybercrime. This model has some advantages in terms of e-commerce, but it does not fix any of the challenges and issues immediately.[3]

The IT Act is regarded as a hazy statute since the scope of regulation in the sense of the internet is vague. Computer forensics is gaining importance in the field of cybercrime evidence investigation because, while evidence is tangible in the real world, it is difficult to expunge information from a computer system in the virtual world of cyberspace. To handle this, computer forensics requires an efficient and knowledgeable computer expert because any carelessness leads to the loss of evidence.

About the fact that the IT (Amendment) Act 2008 addresses further issues, the IPC does not use the word "cybercrime" at any time. Since the year 2008, there has been a surge in cybercrime as hackers find loopholes in the legislation and use them to

[2] Yougal Joshi and Ananda Singh, "A Study of Cyber Crime and Security Scenario",International Journal of Engineering and Management Research, vol.3 (3) June, 2013, pp.13-18.

[3] Ravikumar S. Patel and Dr.DhavalKathiriya, "Evolution of Cybercrimes in India" International Journal of Emerging Trends & Technology in Computer Science, vol.2 (4) July – August 2013.

carry out illicit activities. Cybercrime may be used to harm people, goods, or the government. There are few court precedents to refer to, and old statutes didn't always suit the offense at hand. There is a pressing need to enforce cyber rules. Our scheme can have harsh penalties to serve as a barrier to any illegal activities.

The IT Act (amendment) of 2008 broadened the scope of cyber law. The meaning section of the Proof Act has been changed. The problem of territorial sovereignty is a big one that the IT Act of 2000 does not adequately resolve. It is commonly observed that investigators stop taking cases on the basis of jurisdiction.[4] India's development has not been realized in all aspects, including E-courts, online dispute resolution, good cyber law, cyber forensics, and so on. The Information Technology Act has to be updated. In addition, science and academic professional preparation for lawyers should be made available in India.

Cybercrime is a new form in crime that has the potential to destroy any area of life because it is simple to commit but extremely difficult to find and trace in terms of jurisdiction, considering the geographical indeterminacy of the internet.[5]

To protect the emerging ICT, Cyber Security is needed. The advisory group should identify and suggest a good combination of options for vital ICT structures that complement the nation's governance framework. Understanding the cyber challenge and improving offensive capabilities in this cyber environment is a must. Nations, non-state entities, jihadists, organisations, and individuals are all posing a threat to development, which is becoming increasingly reliant on the cyber domain, necessitating the identification of technologies in this region.[6]

An adversary is an individual who commits a malicious act. Outsiders and insiders will also be adversaries. Insiders are not the same as outsiders. An insider is a person who has been granted access to a nuclear reactor or other classified operations. They were praised for their legitimacy, which included the ability to win admission. Cybercrime is a multibillion-dollar epidemic, and in order to realize the full potential of the computer era, appropriate legislation is needed to prevent overshadowing.

Governments and businesses all over the world are concerned with cyber security. Cyber-threats can take the form of cyber-attacks, but they can also occur as a result

[4] Talwant Singh, "Cyber Law and IT" pp. 1-4

[5] Rohitk.Gupta, "An Overview of Cyber laws vs. Cybercrimes: In Indian Perspective", 2013.

[6] Rohit k Gupta, "An Overview of Cyber law vs. Cybercrimes", 2013.

of “mistakes” or natural disasters. As a result, in the context of cyber security, a specific solution to the specific problem is needed. In cyberspace, there are many problems to be discussed, including data security legal issues, a plethora of spans, cloud infrastructure legal issues, mobile law challenges, and social media legal issues. To keep fraudsters at bay, the builders must go beyond and beyond, and this should be the responsibility of three parties: (1) the king, authorities, and lawmakers; (2) the internet and network service provider or bank; and (3) the internet and network service provider or bank. (3) the individual, in their respective roles, to be responsible for information security.[7]

1.4CYBER LAWS

The 20th century introduced new requisites and offenses to the law glossary. Legal provisions should provide assertion to users, enforcement agencies and deterrence to criminals as it is very important to understand that computer cannot commit a crime but act of people. It is the human beings, not machines, who abuse, demolish and distort information. By realizing the need to combat with the cyber violations, the UNCITRAL, i.e. the United Nations Commission on International Trade Law adopted the Model Law of Electronic Commerce in 1996.[8] It was followed by the General Assembly of United Nation’s recommending that all states should give favourable considerations to the State Model law. In discharge of its responsibility, Government of India also accepted the need to legislate and has approach with the new legislation Information Technology Act, 2000. It was amplified by its amendments. The major acts, which got amended after enactment Information Technology Act, are Indian Penal Code (e.g. 192, 204 ,463, 464, 468 to 470, 471, 474, 476 etc) prior to enactment of IT Act, all evidences in a court were in the physical form only after existence of IT Act, the electronic records and documents were recognized. The Act essentially deals with the following issues:

- Legal identification of Electronic document.
- Legal identification of Digital Signatures

[7] PrabhatDalei and TannyaBrahme, “Cyber Crime and Cyber law in India: An Analysis”‘International journal of humanities and Applied science’ Vol.2 (4), 2014.

[8] Aashish Kumar Purohit, “ Role of Metadata in Cyber Forensic and Status of Indian Cyber Law”, International Journal of computer technology application, vol.2(5) sepoct, 2011.

- Offenses and Contraventions Justice
- Dispensation Systems for cybercrimes.

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cybercrimes as from the prospective of E-Commerce in India, IT act 2000 contains many positive aspects like companies shall now be able to carry out E-Commerce using Legal Infrastructure for the authentication and origin of electronic communication through digital signatures. However, it is considered the ambiguous law in the area of jurisdiction in the context of the Internet. As sec 1 (2) provides that the act shall extended to the whole of India and save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person. Similarly, sec 75 (2) provides that this act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves computer, computer system or computer network located in India. This type of provision appears tobe against the principle of justice. In fact, the term 'cybercrime' at any point even after the amendment by the IT Act Amendment 2008. There is need to push the cyber laws.[9]

1.5 VARIOUS ISSUES UNDER CYBER LAW ENFORCEMENT

Issues related with law

- Territorial jurisdiction is not satisfactory in IT act as jurisdiction has been mentioned in sec 46, 48, 57 and 61 in context of adjudication process and the appellate procedure connected with and again in sec 80 and a part of the police officer power to enter, search a public place for a cybercrime etc. Since the cybercrime are basically computer based crimes and therefore if the mail of someone is hacked in sitting on one place by accused sitting on another Place far in another state, which police station will take the cognizance is difficult to determine because generally investigators avoid accepting complaints on such grounds of jurisdiction.[10]
- Contrary to the real world crimes where tangible evidence in form of weapon of crime, finger prints etc are easy to find and present in court but it is difficult

[9] M.M.Chaturvedi, M.P.Gupta and Jaijit Bhattacharya "Cyber Security Infrastructure in India : A Study" pp.1-15
[10] IDSA Task Report, "India's cyber security challenged" March, 2012

in virtual world to expunge the information from the computer system that what is generally contemplated. This is done with the help of the computer forensics. And the process of preservation of cyber crime evidence lies with the knowledgeable computer forensic expert because any carelessness in the process can lead to diminutive value of the evidence. But it is vital by victim to inform the law enforcement agency as early as possible.

- Experts not only be knowledgeable but also be provided with the technical hardware and software so that they can efficiently fight the cyber crime.
- Law enforcement officers are lack of tools as the old laws are not capable for the crime being committed in the current scenario, new laws hadn't quite caught up to what was happening.
- There is lack of cooperation between the law enforcement agencies and computer professionals.
- The IPC doesn't reveal a term 'cyber crime' at any point even after the IT (amendment) act 2008.
- Lack of security concern in the telecom industry which is integrated into cyberspace, having advert effect of Internet protocol on mobile devices which is considered to be the primary factor for increasing number of attacks.
- Unlike other statutes, policies which are passed by the Indian legislation are not enforceable or binding but merely provide the guidelines for a standard operating procedure. In this regard NCSP doesn't maximize its potential for optimum benefit.

Issues related with the technology

New technology like cloud computing is big concern of cyber threat as for the purpose e-governance and storing data cloud computing is used. The measures taken are not successful to face challenges and risk of cloud computing like:

- Risk of inappropriate access to personal and confidential information.
- Risk of compromise of confidential information and intellectual property
- Appropriate privacy and security measures need to be in place.

Another emerging technology, which is highly in use, is Big Data has critical security and privacy issues. From point of business many works have been carried out focusing on business, application and information processing from Big Data. It's facing many challenges, such as efficient encrypted and decryption algorithms, encrypted information retrieval, reliability and integrity of Big Data.

1.6FUTURE SCOPE

After going through all these issues and ideology, one can hope that in future some hard and fast laws will be implemented to such crimes so that with the increase in the quantum of punishment, new laws for reference, laws with the specific approach to particular problem, making the individual majority of punishment non bail-able, will help to diminish the rate of cybercrime and the era of technological advancement and digitalization can be free from evil.[11]

With the evolving wave in cybercrime, it is critical to have a cyber law enforcement momentum and cybercrime has the potential to destroy any area of life and it is simple to conduct but very difficult to track. Though India has a highly comprehensive and well-defined legal framework, all of the laws in force in the country were passed long ago, taking into account the particular political, social, economic, and cultural circumstances of the time. Nobody could imagine the Internet at the time. Regardless of our master draftsmen's genius skills, the demands of cyberspace could never be expected. As a result, the Internet's arrival ushered in a slew of delicate legal questions and ills, necessitating the adoption of Cyber rules. Second, even with a liberal analysis, the current legislation should not be viewed in the context of the new cyberspace. The Internet necessitates a legal infrastructure that is compatible with the times. Since current regulations have struggled to provide this legal infrastructure, only the introduction of applicable Cyber laws will provide it. Both of these factors combined to create a favorable environment for India to enforce appropriate cyber laws.

1.7LET'S SUM UP

In this chapter, we have learned the issues with respect to cyber law in India. We have also analysed the legal provisions and how there is lack of enforcement leading to higher number of crime rates. We have also learned about the future scope of the said matter.

[11] David Satola and Henry L.July, "Towards a Dynamic Approach to Enhancing International cooperation and collaboration in Cyber Security Framework", 'The MW. Mitchell law journal'.

1.8FURTHER READING

- Rohitk Gupta, “An Overview of Cyber laws vs. Cybercrimes: In Indian Perspective”, 2013. [6]Rohit k Gupta, “An Overview of Cyber law vs. Cybercrimes”, 2013.
- PrabhatDalei and TannyaBrahme, “Cyber Crime and Cyber law in India: An Analysis” ‘International journal of humanities and Applied science’ Vol.2 (4), 2014.
- Aashish Kumar Purohit, “Role of Metadata in Cyber Forensic and Status of Indian Cyber Law”, International Journal of computer technology application, vol.2(5) Sep-Oct, 2011.
- M. M. Chaturvedi, M. P. Gupta and Jaijit Bhattacharya “Cyber Security Infrastructure in India : A Study”pp.1-15 [10]IDSA Task Report, “India’s cyber security challenged” March, 2012
- Angshuman Jana and Kunal Kumar Mondal, “A survey of India Cyber Crime and Law and its prevention approach” ‘International journal of Advance Computer Technology’.
- David Satola and Henry L. July, “Towards a Dynamic Approach to Enhancing International cooperation and collaboration in Cyber Security Framework”, ‘The MW. Mitchell law journal’.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Mention the risks involved with cloud computing.

Following are the issues related to cloud computing-

- Risk of inappropriate access to personal and confidential information.
- Risk of compromise of confidential information and intellectual property
- Appropriate privacy and security measures need to be in place.

2. Explain cybercrime.

Cybercrime is divided into two categories and defined thus-

(a) Cybercrime in a narrow sense that is computer crime in which any illegal behaviour done by the means of electronic operations that targets the security of computer systems and the data processed.

(b) Cybercrime in a broader sense, which is computer related crime any illegal behavior committed by means of an operating system or network, including such crimes as illegal possession or distributing information by means of a computer system or network.

1.10ACTIVITY

Reflect upon the legal provisions in relation to cyber law in India. (Word count- 2000 to 2500)

Unit 2: EMERGING TRENDS IN CYBER CRIMES IN INDIA: AN OVERVIEW

2

Unit Structure

2.1 LEARNING OBJECTIVES

In this chapter we will learn-

- The challenges under cyberspace and various types of cyber crimes
- Various modes and manners to commit cyber crime
- Legal provisions to regulate cybercrime.

2.2INTRODUCTION

Computers and the internet have been an indispensible feature of our lives. Individuals and cultures use them to make life better for themselves. They use them for nearly every part of life, including saving documents, processing data, sending and receiving messages, correspondence, operating computers, typing, editing, painting, and drawing. Cybercrime is described as "unlawful actions in which a computer is used as a weapon, a target, or both". In the internet, there are several different types of offences. Some aren't dangerous enough to be classified as a felony, but are just a means of disseminating information. They are merely a display of abilities and are completely harmless. When man created the machine and developed the infrastructure for interacting with machines, he would never have imagined that the virtual space he was building would be filled with cyber-crime. But, by now, nearly everyone has learned of the words digital crime, cyber-crime, ecrime, hi-tech crime, or electronic crime, which refers to any action carried out in cyberspace with a criminal intent.

In basic terms, it is an illegal offense in which a device or network serves as the cause, weapon, goal, or location of the crime. To put it simply, cyber-crime applies to any actions carried out in cyberspace with the intent of committing a crime, as described by the researchers. Unauthorized access, illegal interception by technical means of non-public transmissions of computer data to, from, or inside a computer system, data interference by unauthorized damaging, deletion, deterioration, alteration, or suppression of computer data, and systems interference by interfering with the functioning of a computer are all examples of such crimes involving an information technology infrastructure. In today's e-Age, "crime" has expanded beyond physical abuse and psychiatric torture to include our online lives. Our lives and surviving in the cyber universe is referred to as E-Life.

Since computers and the internet have become an important part of our personal and professional lives, we are all a part of this cyber universe, whether directly or indirectly. Computers and the Internet, like any other technology, are a blessing to humanity if used correctly and to the benefit of society; otherwise, they are a curse. But, as we all know, everything has advantages and disadvantages, and computers and the internet are no different. If we understand 'Cyber Crime' to be a virus, it is reasonable to conclude that this virus is corrupting man's major creation (computers and the internet), which is responsible for the development of a decent civilization for men. Cybercrime is a global threat that is one of the most difficult and difficult to identify and prosecute. It's worth noting that the official website of the Crime Branch Mumbai's Cyber Crime Investigation Cell notes, "The unseen suspect is more dangerous than the visible criminal."[12]

2.3REASONS FOR CYBER CRIMES

H.L.A. Hart in his work "The Concept of Law" has said 'human beings are vulnerable, so rule of law is required to protect them'.3 Applying this to the cyberspace, we may say that computers are vulnerable, so rule of law is required to protect and safeguard them against cybercrime. Some reasons for the vulnerability of computers are given as under:[13]

1. *Capacity to Store Data in Comparatively Small Space*: The computer has unique characteristic of storing data in a very small space. This makes removing or deriving information either through physical or virtual medium much easier.

2. *Easy Accessibility*: The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers can steal access codes, advanced voice recorders, retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

3. *Complexity:* Computers are regulated by operating systems, which are made up of millions of lines of code. The human mind is fallible, and there would almost always

[12] www.newsnish.com/technology/websocial

[13] Nations prepare for cyber war, By David Goldman@ CNN Money Tech, January 7, 2013. http://money.cnn.com/2013/01/07/technology/security/cyber-war/index.html

be a lapse at some stage. Cyber criminals may exploit these flaws to gain access to the computer system.

4. *Negligence:* Negligence is very closely connected with human conduct. It is, therefore, very much probable that while protecting the computer system, there might be any negligence, which, in turn may provide a cyber-criminal an opportunity to gain access and control over the computer system.

5. *Loss of Evidence*: Loss of evidence is a very common & obvious problem as all the data is prone to get destroyed further collection of data outside the territorial extent also paralyses the system of crime investigation.[14]

2.4 MODES AND MANNERS OF COMMITTING CYBER CRIMES

1. Unauthorized Access to Computer Systems: In the broadest context, this kind of crime is referred to as hacking. However, in order to prevent any misunderstanding, the framers of the Information Technology Act of 2000 used this phrase. We wouldn't use the words hacking and unauthorized access interchangeably because the latter has a broader meaning.[15]

2. Theft of Information Contained in Electronic Form: This covers data stored on computer hard drives, portable storage media, and other similar devices. Theft may occur either by physically misappropriating data or by interfering with it through any virtual means.

3. Email Bombing: This kind of activity refers to sending large number of emails to the victim, which may be an individual or a company or even mail servers .This targets at ultimately crashing of the system or the data.

4. Data Diddling: This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is complete. The electricity board faced a similar problem of data diddling while the department was being computerized.

5. *Salami Attacks*: This type of crime is commonly seen in financial institutions and is carried out with the intent of committing financial crimes. A key characteristic of this form of crime is that the change is so minor that it will usually go unnoticed, such as

[14] CYBER WARFARE - Institute for Security Technology Studies. www.ists.dartmouth.edu/docs/cyberwarfare.pdf Similar

[15] http://idsa.in/system/files/book_indiacybersecurity.pdf

in the Ziegler example, where a logic bomb was planted in the bank’s system, deducting 10 cents from each account and depositing it in a specific account.

6*. Denial of Service Attack*: In this scenario, the victim’s computer is inundated with more requests than it can accommodate, causing it to fail. A distributed denial of service attack is a form of denial of service attack in which the perpetrators are targeted in large numbers and over a large geographic area. Amazon and Yahoo, for example.

7. *Virus Attacks:* Viruses are computer programs that bind themselves to a computer or a file, and spread to other files and devices on a network. They normally have an effect on a computer’s data by modifying or removing it. Unlike viruses, worms do not need a host to bind themselves to. They simply make working copies of themselves and replicate the process until they have consumed all of the available memory on a computer, such as the love bug virus, which infected at least 5% of the world’s computers. The damages were estimated to be in the amount of $ 10 million. The Internet worm, which was released on the Internet by Robert Morris sometime in 1988 and almost bringing the Internet to a halt, is the world’s most popular worm.

8*. Logic Bombs:* There are programs that are triggered by events. This means that these systems are designed to act only when a certain occurrence (referred to as a trigger event) happens. Some viruses are referred to as logic bombs because they are inactive for the majority of the year and only become operational on a certain day (like the Chernobyl virus).

9*. Trojan Attacks:* This phrase comes from the word “Trojan horse.” This is a term used in the software industry to describe an illegal program that assumes passive influence of another device by posing as an approved program. The most popular method of Trojan installation is by e-mail; for example, a Trojan was installed in the machine of a female film director in the United States while speaking.

10. Internet Time Thefts: The victim’s Internet browsing hours are usually taken up by another user in these types of robberies. This is accomplished by getting access to the login ID and password, for example, in Colonel Bajwa’s case, the Internet hours have already been taken up by someone else. This was perhaps one of the first cases of cyber-crime in India to be published. The police, on the other hand, were embarrassed by this case because of their lack of knowledge of the existence of cyber-crime.

2.5CYBER CRIME AND SECURITY

Apart from the dangers of increasing police powers, relying on prosecutors to plan and implement solutions in a highly technical area in which private control is regarded as a substantial advantage may well be ineffective even in satisfying the need for better security. Those who support adoption of a multilateral approach to deal with this quintessentially transnational problem must be encouraged by the fact that states have consistently adopted by the fact that states have consistently adopted multilateral solutions to deal with technologies that affect populations across national boundaries.[16] As technology advances, new technologies with sensational impact that require transnational controls have repeatedly led to multilateral arrangements; agencies have been created to deal with such international areas as air travel, shipping and telecommunication. Transactional needs have demanded transition salutation, which have been satisfied through international agreements on principles, standards, and practices, often developed and proposed by specialized international agencies. States make such arrangements based not upon ideological consideration but on considerations of safety, productivity, and efficient. They have done so, moreover, with no sacrifice of national sovereignty, and almost entirely on the basis of consensus decisions determined by both self -interest and reciprocity.

The information infrastructure faces analogous challenges. Its security and efficiency will be materially increased through international implementation of principles, standards and practices specially designed for this field of activity. The optimum manner of achieving these objectives in this particular field is a multilateral treaty with the necessary commitments to cooperate in investigating and prosecuting an agreed range of conduct, and an international agency with authority to accomplish the legal and technological objectives essential to create a more secure cyber world.

2.6CYBER WARFARE

While there is no universally accepted concept of cyber warfare, it has been observed that states could be attacking other countries' computer systems for

[16]"Statement for the Record of Guadalupe Gonzalez, Special Agent in Charge, Phoenix Field Division, FBI on Cyber crime" before the Special Field Hearing, Senate Committee on Judiciary, Subcommittee on Technology, Terrorism, and Government Information, Washington, DC

espionage and to destroy their sensitive infrastructure. It mostly applies to politically motivated hacks for sabotage and spying purposes. It is a type of information warfare that is often compared to conventional warfare, though this comparison is debatable in terms of precision and political motive. The assaults on Estonian and Georgian websites in 2007 and 2008 were widely publicized.[17]

While there is no conclusive proof of a state's participation in these attacks, it is generally assumed that non-state actors (such as hackers) were used by state actors. Since these cyberattacks, the topic of cyberwarfare has gained prominence in the international press. The United States has acted quickly to establish a cyber command within the Strategic Forces Command and to update its military doctrine. After ground, air, seas, and space, the US has proclaimed cyberspace to be the fifth dimension of warfare, and has claimed the right to take any action, including nuclear strikes, in response to cyberattacks against it, according to the most recent official military doctrine. Other countries are almost likely to react by following identical military doctrines. The controversy about whether cyber attacks qualify as acts of violence and whether international law on warfare extends to cyber warfare is raging. The question of whether or not there should be codes of conduct for state actors in cyberspace is being debated at the multilateral level.

Since cyberattacks can't be traced back to a single individual, and they affect different computer networks in multiple countries, the problem gets incredibly complicated. The idea of cyber deterrence is still being questioned, but it's unclear if it will work in cyberspace given the ease at which non-state actors can get involved and the lack of attribution. However, there is a continuing controversy between those who think electronic warfare is over-hyped and those who believe the planet is on the verge of a cyber Armageddon.[18]

Both sides have good points, but cyber warfare as a concept has become unavoidable as the number of countries establishing cyber commands continues to rise. These orders have been supplemented by attempts to establish military theories that are applicable. As a result, there is an urgent need to consider electronic warfare rules, whether the rules of armed conflict (LOAC) should be applied to cyber warfare, and how concepts like proportionality and neutrality apply

[17] "Cyber attacks rise from outside and inside corporations", Press Release from Computer Security Institute.

[18] "Ninety percent of survey respondents detect cyber attacks, 273 organization report $265, 589, 940 in financial losses", Press Release from Computer Security Institute, March 22, 2000

in the cyber realm. In the light of cyber warfare, current collective security laws such as Article 41 of the UN Charter and Chapter 7 are considered lacking, especially in terms of the rapidity of cyber-attacks and the excessive time it takes for decision-making and action under these rules.

2.7LET’S SUM UP

In this chapter, we have learned about the types of cybercrimes and various measures to tackle the same. Besides, we also understood the dimension of cyber security in India along with its related relevant provisions.

2.8FURTHER READING

- Noack, David. Computer Viruses Cost $12 Billion in 1999”, APB News, Jan. 20, 2000 5. 2. “Love Bug Damage Costs Rise to $6.7 Billion” Press release by Computer Economics, May 9, 2000.
- “Statement for the Record of Guadalupe Gonzalez, Special Agent in Charge, Phoenix Field Division, FBI on Cyber crime” before the Special Field Hearing, Senate Committee on Judiciary, Subcommittee on Technology, Terrorism, and Government Information, Washington, DC
- Noack, David. “Businesses Use $12 Billion of Stolen Software” APB News, May 25, 2000, 8. Salkeyer, Alex. “Who Pays When a Business Is Hacked?” Business Week Online: Daily Briefing, May 23, 2000.
- “Cyber attacks rise from outside and inside corporations”, Press Release from Computer Security Institute.
- “Ninety percent of survey respondents detect cyber attacks, 273 organization report $265, 589, 940 in financial losses”, Press Release from Computer Security Institute, March 22, 2000
- Howe, Carl; McCarthy, John C.; Buss, Tom; and Davis, Ashley. “The Forrester Report: Economics of Security”, February, 1998
- Webster’s Third New International Dictionary, Merriam-Webster, Inc., Springfield, MA, 1986, page 2442.

2.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is cyber warfare?

While there is no universally accepted concept of cyber warfare, it has been observed that states could be attacking other countries' computer systems for espionage and to destroy their sensitive infrastructure. It mostly applies to politically motivated hacks for sabotage and spying purposes.

2. What is internet theft?

The victim's Internet browsing hours are usually taken up by another user in these types of robberies. This is accomplished by getting access to the login ID and password, for example, in Colonel Bajwa's case, the Internet hours have already been taken up by someone else. This was perhaps one of the first cases of cyber-crime in India to be published. The police, on the other hand, were embarrassed by this case because of their lack of knowledge of the existence of cyber-crime.

2.10ACTIVITY

Reflect upon the types cybercrimes and legal provisions in relation to cyber law in India. (Word count- 2000 to 2500)

Unit 3: STUDY OF LATEST EMERGING TRENDS ON CYBER SECURITY AND ITS CHALLENGES TO SOCIETY

3

Unit Structure

3.1 LEARNING OBJECTIVES

In this chapter we will learn-

- Latest trends on cyber security
- The concerns and measures taken by government.
- Various challenges to the society.

3.2 INTRODUCTION

The Internet is one of the most rapidly developing fields of technical technology. Disruptive innovations such as cloud analytics, social computing, and next-generation mobile computing are radically transforming how businesses use information technology to share information and perform business digitally in today's business world. Since more than 80% of all commercial transactions are now conducted electronically, this area necessitated a high level of protection to ensure transparent and efficient transactions.[19]

Cyber Defense encompasses not just the security of IT applications within the enterprise, but also the wider digital networks on which they depend, such as cyberspace and sensitive infrastructures. In the continuing advancement of information infrastructure and Internet services, cyber security plays a critical role. Enhancing cyber protection and safeguarding sensitive information infrastructures are critical to the security and economic well-being of every nation. Making the Internet better (and protecting Internet users) has been a key component of both new service creation and government policy.A national cyber security and sensitive information infrastructure defense policy would provide measures to deter cybercrime.

As a result, developing and implementing a national policy and plan for cyber defense necessitates a multifaceted approach. Cyber security measures, such as the implementation of technical defense mechanisms or consumer education to discourage them from being victims of cybercrime, can help to reduce cybercrime risk. In the battle against cybercrime, developing and implementing cyber defense solutions is critical.

[19] Anderson, Boehme, Clayton, Moore. (2008). Security Economics and the Internal Market. Available: http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec.

The war against cybercrime necessitates a multifaceted strategy. Given that technological solutions alone cannot deter any crime, law enforcement authorities must be able to successfully detect and prosecute cybercrime.[20]

3.3LATEST ISSUES ON CYBER SECURITY

Privacy and identity theft will remain the most pressing security concerns for businesses. We exist in an environment where all data is stored digitally. Users can connect with friends and relatives in a secure environment on social networking sites. Cybercriminals will continue to hack social media platforms to harvest personal data from home users.[21] There will be new attacks on Android-based smartphones, but they will not be on a large scale. Since tablets and smart phones use the same operating system, they will soon be infected with the same malware as those devices. The number of malware specimens for Macs will continue to rise, but at a much slower rate than for PCs. Windows 8 would enable developers to create apps on almost every Windows-based computer (PCs, laptops, and smart phones), making it easier to create malicious applications similar to those for Android.[22]

Any other day, we hear about cyber-threats such as malware, phishing, and IoT-based attacks. However, enterprises must be mindful that 2020 will bring a whole new level of cybersecurity risks. According to a study by Threat Horizon, organisations will face cyber attacks in the coming years under three main themes –

- Disruption: Relying too much on shaky infrastructure increases the likelihood of planned internet outages that jeopardize business operations. Ransomware can be used by cybercriminals to take control of the Internet of Things.
- Knowledge Distortion: The spread of disinformation by bots and artificial sources would jeopardize interest in the quality of data.
- Deterioration: The capacity of an organization to monitor knowledge would be harmed by rapid developments in smart technology and competing demands raised by changing national security.

Cybercriminals are actively searching for new exploits and devising advanced techniques to defraud and damage institutions and organisations in this era of digital

[20] Integrated Defense Staff, “National Informatics Center”, Ministry of Defense, India
[21] Cyber Security Strategy of United Kingdom, 2009
[22] ITU Cyber Security Work Program to Assist Development Countries, 2009

revolution and globalization. In terms of this, companies should be aware of not just the ever-increasing amount of vulnerabilities, but also the looming cybersecurity risks. The details in this post will remind you of the upcoming threats in 2020, allowing you to take preventive steps to mitigate their harm.

3.4RECENT SURVEY ISSUES ON CYBER SECURITY TRENDS

The following list was developed from cyber security research and survey

Mobile Devices and Apps

When the number of mobile devices grows, so does the number of security threats. Any new smart phone, tablet, or other electronic computer adds to the number of insecure access points to networks, making them more vulnerable to cyber-attacks. This tragic dynamic is well-known to thieves, who are prepared to strike with highly targeted ransomware and mobile app attacks. Similarly, the issue of lost and stolen computers will grow to cover these modern and outdated technology that historically went unnoticed by cyber security planners.[23]

Social Media Networking

Personal cyber attacks will increase as the use of social media grows. The use of social media for corporations is on the rise, as is the possibility of attack. Organizations should continue to see a rise in the use of social media accounts as a platform for social engineering strategies in 2012. Companies would need to look beyond simple protocol and practice implementation to more sophisticated capabilities including data leakage protection, improved network management, and log file review to combat the threats.

Cloud Computing

Cloud computing is a new technology that brings different types of services under one roof. Cloud computing provides services over the internet and the client pay according to their usage. Suppose you want to travel from New York to London you do not need to own or purchase a plane. Instead of this you book a ticket and pay for the airline, according to your destination. The rest of the things will be managed by the airline staff. The same working model is adopted by cloud computing. In cloud computing you pay for what you use the rest of the things will managed and

[23] Schjolberg/Hubbard, “Harmonizing National Legal Approaches on Cybercrime”, 2005

maintained by cloud providers. In cloud computing concept different entities play the different role according to its need. These entities system can be multi layer to basic three layer model.

In basic three layer model of cloud computing Consist: Client, Cloud Service Provider and Cloud Host Company.

i. ***Client:*** A Client is an entity that uses the service from the provider to solve their business computing problems. It can be considered as an end user. The Consumer access the provider's service, either through the API or Internet Connection. A cloud consumer is charged on the basis of usage according to Pay-per-use Model.

ii. ***Cloud Service Provider***: A Provider is usually a third party that makes services available for a customer. A cloud service provider working as a bridge between the end user and the cloud Host company. It maintains the required infrastructure and capabilities to deliver service to the customer. The capabilities vary based on the type of cloud service the provider delivers.

iii. ***Cloud Host Company***: An intermediary works on the behalf of Cloud consumers to deal with the provider. It helps the consumer to architect the right system on a cloud provider, and assists in all activities of a provider and consumer.

Cloud storage can be used for more businesses. Cloud computing's huge cost savings and efficiencies are convincing businesses to move to the cloud. Organizations would be able to better handle the challenges of cloud computing if they have a well-designed infrastructure and internal security preparation. Unfortunately, recent polls and studies show that businesses underestimate the value of protection due diligence while vetting these vendors. If the number of people using the cloud grows in 2012,[24] new breach cases will demonstrate the difficulties that these services face for forensic investigation and incident management, and cloud protection will hopefully get the recognition it deserves.

Protect systems rather Information

The emphasis will be on information security rather than machine security. As customers and companies increasingly store important information electronically,

[24] ArunPrabhudesai, "Cyber Attacks In India", 2011

protection considerations can expand from merely handling systems to securing the data these systems contain. Rather than concentrating on designing processes to secure the databases that store information, consumers and businesses would require more granular control of the data stored there.

New Platforms and Devices

Cybercriminals would have additional openings as a result of new platforms and computers. Personal computers running Windows have long been concerned with security risks. However, the introduction of emerging platforms and smart phones - such as the iPhone, iPad, and Android - would almost certainly result in new challenges. This summer, the first Android phone was infected with a Trojan, and rumors of malware software and spyware continue to surface, not just on Android.[25]

Everything Physical can be Digital

Printed notes on a sheet of paper, journal binders, and even pictures on the wall can be copied in digital format and gleaned for the tools to enable an activist-style security breach, and this will become increasingly a challenge.

3.5PRACTICES AND CONCERN BY GOVERNMENTS FOR CYBER SECURITY

Ensure the national cyber security strategies take into account the interests of all people, not just those of central government. Encourage adoption and implementation of the Cybercrime Convention and other proposed international treaties. Support end-user education because it not only supports the actual user and scheme, but it also decreases the amount of vulnerable machines that can be hijacked by hackers and used to launch assaults. Influence computer industry vendors to supply professionally validated hardware and applications by using procurement control, standard-setting, and licensing. Increase the number of specialized police and forensic computing services available. As the most likely way of averting or mitigating a large-scale Internet crisis, support the international Computer Emergency Response Team (CERT) group, even by funding. Strengthened Internet protocols, Risk Analysis, Contingency Planning, and Disaster Propagation Analysis, Human Factors in the Use of Computer Technology, and Security Economics are all fields where research is required.

[25] GAO (2010), Cyberspace, United States faces Challenges in Addressing Global Cybersecurity and Governance, GAO-10-606 http://www.gao.gov/products/GAO-10-606

3.6SPECIFIC CYBER SECURITY TECHNOLOGIES

Access Control and Identity Management - The username/password combination has been a fundamental of computer access control since the early 1960s.[26]

Authentication- Documents need to be authenticated as having originated from a trusted source and that they have not been subsequently altered.

Malware scanners-Software that is regularly scans files and messages for malicious code.

Firewalls- A firewall program will monitor traffic both into and out of a computer and alert the user to apparent unauthorized usage.

Cryptography-It is used in information management in two ways. The more well-known method is to provide secrecy by encrypting all saved and transmitted data.

3.7POSSIBLE COUNTERMEASURE TECHNIQUES

Users and organisations will improve their preparation and response to better protect against a variety of threats and mitigate the possible impacts of attacks by following good cyber protection practices:[27] Make sure your smart phones and other electronic devices have encryption and password features available. Configure and patch operating systems, browsers, and other device applications correctly. Firewalls, anti-virus, and anti-spyware applications can all be included and modified on a daily basis. Always be careful when communicating with others; deliberate before you press. On social media platforms, don’t share too much personal knowledge about yourself. You may become a victim of identity theft or property theft depending on the details you share. When unauthorized contact or actions are discovered, report them to Internet service providers and local law enforcement.

3.8KEY CHALLENGES TO SOCIETY

Public and private agencies in the fields of public health, emergency care, administration, defense industrial base,[28] information and telecommunications, electricity, transportation, banking and finance make up our nation’s vital infrastructures. India’s dependence on technology is also reflected in the fact that the

[26] Information Warfare Monitor (2010), Shadows in the Cloud, www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2- 0

[27] Mukhopadhyaya, K and Sinha, B P. (1992). Reliability analysis of networks using stochastic model . Information Sciences . Volume 65, Issue 3, 225-237 .

[28] OECD (Organisation for Economic Cooperation and Development) (2002), OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Recommendation of the Council adopted 25 July 2002, OECD, Paris.

country is changing gears by dabbling in e-government. India has now embraced e-government in areas such as income tax and passports and visas. Sectors such as law enforcement and the courts will be followed. This is indeed a big deal in the tourism industry. The majority of Indian banks have completed full computerization. E-commerce and e-banking have since been introduced as a result of this. The financial markets haven't been spared yet.

Cybercrime has evolved into an extreme, pervasive, violent, rising, and increasingly advanced threat to national and economic security. Many businesses, institutions, public and private-sector entities (especially those involved in essential infrastructure) are in grave danger. Having the Cyber Security stance correct around the board would be critical for future growth, creativity, and competitive advantage for both companies and governments. Businesses will be able to work for a potential world that is both transparent and stable and prosperous by collaborating through public and private sector alliances and advancing security policies, especially with regard to mission-critical networks, procedures, and technologies that are linked into cyberspace.

3.9LET'S SUM UP

In this chapter, we have learned various terminologies including cloud computing, data protection, social media networking etc. Additionally, we have analysed latest trend on cyber security and its interface with possible countermeasure techniques.

3.10FURTHER READING

- Integrated Defense Staff, "National Informatics Center", Ministry of Defense, India
- Yang, Miao, "ACM International Conference Proceeding Series", vol. 113
- Unisys Corporation, "Unisys Descriptive Technology & Trends Points of White Paper Series- Cyber Security" USA, 2011
- Cyber Security Strategy of United Kingdom, 2009
- ITU Cyber Security Work Program to Assist Development Countries, 2009, Rev. Jonames Burg, TTU WTSA Resolution 50, 2008
- ITU Cyber Security Work Program to Assist Development Countries, 2008
- Kellermann, "Technology Risk Checklist, Cybercrime and Security", IIB-2

- Schjolberg / Hubbard, “Harmonizing National Legal Approaches on Cybercrime”, 2005
- The most Important Instruments in fight against Cybercrime, Ch. 6.2
- Luis Corrons, Technical Director, Panda Labs, Bangalore, 2012
- ArunPrabhudesai, “Cyber Attacks In India”, 2011
- Audry Watters, Read Write Cloud, RWW Solution Series, 2010

3.11CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Explain the scope of Cyber security.

Cyber Defense encompasses not just the security of IT applications within the enterprise, but also the wider digital networks on which they depend, such as cyberspace and sensitive infrastructures. In the continuing advancement of information infrastructure and Internet services, cyber security plays a critical role. Enhancing cyber protection and safeguarding sensitive information infrastructures are critical to the security and economic well-being of every nation.

2. Highlight latest cyber security issue.

There will be new attacks on Android-based smart phones, but they will not be on a large scale. Since tablets and smart phones use the same operating system, they will soon be infected with the same malware as those devices. The number of malware specimens for Macs will continue to rise, but at a much slower rate than for PCs. Windows 8 would enable developers to create apps on almost every Windows-based computer (PCs, laptops, and smart phones), making it easier to create malicious applications similar to those for Android.

3.12ACTIVITY

Elaborate specific cyber security technology along with its interface with latest trends. (Word count- 2000 to 2500 words)

Unit 4: CHALLENGES TO ENFORCEMENT OF CYBER-CRIMES LAWS AND POLICY

4

Unit Structure

4.1 LEARNING OBJECTIVES

In this chapter we will learn-

- Reasons for committing cybercrimes.
- Various challenges in enforcement of cybercrime.
- Legal provisions/statutes with respect to the regulation of cyber crime.

4.2 INTRODUCTION

Cyber-crimes are a relatively new phenomenon, but they have become the focus of global attention simply because all citizens of the world, whether private or public, are vulnerable to them. This vulnerability is almost unavoidable because the world is in an information age (Encyclopaedia of Library and Information Science, 1977), and cyber-crimes emerged with the advent of the internet. To begin, it is important to make a brief distinction between a computer crime and a cyber-crime, the reason being that the two terms are often confused as one and the same, when in reality they are just identical but distinct.[29]

Computer crimes are crimes committed using a device; in other words, computer crimes include crimes committed against the computer hardware, the materials contained or connected with the computer, such as software and data; common examples of computer crimes include embezzlement, theft, financial manipulation, and hacking, among others. Cyber-crime is a catch-all word for two types of crimes: cyber-dependent and cyber-enabled (McGuire and Dowling, 2013). Cyber-dependent crimes are those that can only be committed through the use of a data, computer networks, or some means of ICT.[30]

The definitional problem of cybercrime persists, yet one thing is certain: most definitions of cybercrime make reference to the Internet; for the sake of overcoming the dichotomies in jurisdictions and still addressing the same concept in legal literature, cybercrime has no globally accepted definition that might possibly encapsulate all the facets of this novel brand of crime.Cybercrime, according to the

[29] Ahamad M, Amster D, Barrett M, Cross T, Heron G, Jackson D, King J, Lee W, Naraine R, Ollmann G, Ramsey J, Schmidt HA, Traynor P (2008). Emerging Cyber Threats Report for 2009, Georgia Tech Information Security Centre. Georgia Inst. Technol. 9p.

[30] Ajayi EFG (2016). The Impact of Cybercrimes on Global Trade and Commerce. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2810782 or http://dx.doi.org/10.2139/ssrn.2810782

Oxford Dictionary of Law (2002), is any criminal or other offence that is encouraged by or involving the use of electronic media or computer networks, such as any computer or the Internet, or any one or both of them.

4.3MOTIVATIONS FOR CYBERCRIME

Such cybercrime consequences include but are not limited to loss of intellectual property and sensitive data, cost of opportunity including service and employment disorder, brand image and company reputation, penalties and compensatory payments to clients, in addition to the global financial losses outlined in the paragraphs above (Paganini, 2013).After highlighting the impact of cybercrime in terms of financial and economic impacts,[31] as well as other repercussions, the appropriate concern that will inevitably agitate the mind of a thoughtful individual is: what are cybercriminals' motivations?

The following is a brief response to this important issue: The profit motive seems to be the first and most important motivation for cybercriminals to continue their nefarious activities of infiltration or unauthorized interference with computers and network systems; the profits accruing to cybercriminals are enormous; as previously said, the financial losses at the global level are profits to cybercriminals.[32] The difficulty of detecting cybercriminals is closely related to the profit motive; the Internet provides a broad range of freedom for all citizens of the world, and the lack of a requirement of identification as to who is doing what, through the use of telecommunications through cyberspace, continues to thwart global efforts aimed at tracking criminals and bringing them to justice.

Competitors bolster cybercriminal activity by sponsoring attacks on one another, whether by hacking to steal sensitive knowledge about trading secrets or distributed denial of service attacks to cripple a competitor's service (DDoS). It should be noted that certain cybercriminals are motivated solely by the satisfaction or pleasure they derive from gaining unauthorized access to computers and computer networks; the very fact that cybercriminals are able to gain access to computer systems that the owners and operators believe to be safe and secure, thus revealing vulnerability,

[31] Centre for Strategic and International Studies (CSIS) (2014). Net Losses - Estimating the global cost of cybercrime. Economic impact of cybercrime II. June 2014. pp. 1-24. Available at: http://www.mcafee.com/us/resources/reports/rp-economic-impactcybercrime2.pdf

[32] Chang W, Chung W, Chen H, Chou S (2003). An International Perspective on Fighting Cybercrime, ISI'03 Proceedings of the 1st NSF/NIJ conference on Intelligence and security informatics. pp. 379- 384.

gives the cybercriminal a competitive advantage. Finally, a threat or protest against computer networks, which is an external expression of registering disagreement or criticism against owners or administrators, is another type of incentive for cybercriminals. This type of motivation is more often than not directed at profiting from cybercriminal activities.

4.4CYBERCRIME STATUTES

Cybercrime seems to be well known to the ordinary Internet savvy citizen anywhere he is located on the globe; nevertheless, the idea of cybercrime has no universally recognized meaning. Cybercrime, on the other hand, is described as the use of a device with an Internet connection to commit online crimes.[33] In light of the above, this paper defines cybercrime as illicit internet-mediated practices that often occur in global electronic networks (Chang et al., 2003). There are many forms of cybercrimes and for ease of reference, it includes but not limited to 419 emails and letters, advance fee fraud, online auction fraud, online betting fraud, botnet-related fraud, child pornography and related offences, computer hacking, computer related forgery, computer related fraud, cracking, credit card fraud, cyber-laundering, cyber-smearing, cyber piracy, cybersquatti, Trojan horse, spyware, system interference and vishingare only a few examples of cybercrime.[34] Many sovereign countries around the world have policies in place to deter, regulate, criminalize, investigate, and prosecute cybercrime, and those who do not are working to pass regulations to address the threat faced by cybercrime. Hereunder is a summary of measures embarked upon at international and regional levels to address cybercrimes:

In 1997, the G8 released a Ministers' Communiqué outlining an action plan and principles to fight cybercrime and secure data and networks from unauthorized access. It also stated that all law enforcement officers must be prepared and ready to deal with cybercrime, and that all member countries must have a point of touch available 24 hours a day, seven days a week (Chang, 2003). In 1990, the United Nations (UN) General Assembly passed a resolution on electronic crime law. It also passed a resolution in 2000 to curb criminal misuse of information technology, and a

[33] Convention on Cybercrime (2001). Summary of the treaty, European Convention on cybercrime. Available at: ftp://ftp.freenet.at/privacy/gesetze/europarat-cybercrime-summary.pdf

[34] Ernst, Young (2003). Fraud: Unmanaged risk. 8th global survey. Global investigations dispute advisory services, South Africa. Available at: https://www.whistleblowing.com.au/information/documents/EY8thGlobalSurvey2003.pdf

second resolution in 2002 to tackle criminal misuse of information technology (Nicholas, 2008).

The International Telecommunication Union (ITU), which is responsible for telecommunications and cyber security matters at the United Nations, issued the Geneva Declaration of Principles and Plan of Action in 2003, stressing the relevance of interventions in the battle against cybercrime, and in 2005,[35] the Tunis Commitment and Tunis Agenda for the Information Society. In 2001, the Council of Europe (CoE), which comprises 47 European member states, took the lead by establishing the first international Convention on Cybercrime, which was drafted in collaboration with the United States, Canada, and Japan and signed by 46 member states but only ratified by 25. (Ahamad et al., 2008).[36] The Convention, also known as the Budapest Convention, is the first transnational settlement on crimes committed through the Internet and other electronic networks, focusing on copyright infringements, computer-related piracy, child pornography, and network security breaches which also include a number of forces and processes, such as computer network search and interception.

4.5CHALLENGES TO ENFORCEMENT OF CYBERCRIMES

The efforts made by the instrumentality of legislations at national, international, and regional levels were discussed previously; without prejudice to the effectiveness of the existing laws in place to combat cybercrime, the scourge persists, nay, rather than the laws to curb, or better still, minimize cybercrime, there is a rise in the frequency and sophistication of cybercrime, and the reason for this is that cybercrime is becoming more sophisticated. Here, the challenges faced by mankind which makes cybercrimes intractable are discussed as follows:

Identity of cybercriminals

There is no simple way of determining who is doing what and where an Internet user is located at any given time; the global information system is open, and there are no prerequisites that must be met before a user can communicate with others, anywhere on the planet. As a result of the unrestricted freedom of information and

[35] International Telecommunication Union (2009). Understanding Cybercrime: A Guide for Developing Countries, ITU Telecommunication Development Sector. https://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

[36] McGuire M, Dowling S (2013). Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, Home Office, United Kingdom, October. 30p.

correspondence, cybercriminals may conceal their identities using various telecommunications devices, making it difficult to track a user's online Internet Protocol (IP) address. Furthermore, even if a cybercriminal's IP address can be traced to a specific location, the next barrier cannot be overcome because a cybercriminal's identity is unknown to the owner or user of the Internet service provider.

Jurisdictional challenges

Aside from the important problem of privacy previously mentioned, another formidable obstacle to the prosecution of cybercrime legislation is authority. Taking into account the time-tested values of state freedom, autonomy, and territorial integrity, each nation-state in the world has the authority to enact laws that apply to all objects and people within its geographical entity, referred to as a territory. Conflict of laws is inevitable due to the above cause of nation-states passing laws on the same subject from separate jurisdictions. The power of a court or judge to entertain an action, appeal, or proceeding is known as jurisdiction. The question of jurisdiction is so fundamental that it serves as the foundation for every decision, or, to put it another way, it goes to the heart of every case before the courts. A court that lacks authority therefore lacks the requisite competence to hear the appeal. A lack of integrity renders the litigation null and void from the start, regardless of how well-run and settled the case might be.[37]

Extradition processes challenge

The term extradition is made up of two French words: ex, which means "out," and custom, which means "deliverance." That is the method of a new judicial jurisdiction recalling someone convicted of a crime for conviction or punishment. Extradition is often known as the surrender of a person convicted of committing an offense in one state to another (Oxford Dictionary of Law, 2002).A cursory glance at the above definition of extradition might lead one to believe that if a person is accused of committing a cybercrime in one jurisdiction and flees to another, all that is required of the country where the cybercriminal is domiciled is to quickly return the said criminal to the requesting country to face trial; however, in practice, this is not the case.

[37] Nicholas CAMQC (2008). Emerging Trends in Cyber Crime, 13th Annual Conference - New Technologies in Crime and Prosecution: Challenges and Opportunities, International Association of Prosecutors, Singapore. Available at: http://www.odpp.nsw.gov.au/docs/default-source/speeches-bynicholas-cowdery/emerging-trends-in-cyber-crime.pdf?sfvrsn=2

There is no instrument of international law that requires sovereign states to automatically return cybercriminals for prosecution. In effect, countries where cybercriminals are located often fail to extradite cybercriminals for various reasons, and this trend poses an insurmountable obstacle to the global implementation of cybercrime laws.

4.6DEARTH OF EXPERTS IN PROSECUTION OF CYBERCRIMES

The lack of expertise in the investigation of cybercrimes is linked to the above causes of insufficient experience, remuneration, and inadequate security and safety on the dangerous job for law enforcement agency officers. It is a well-known fact that, even though law enforcement agencies did a good job investigating cybercrime,[38] at the litigation stage, the expertise of prosecution attorneys is also critical in securing the conviction of a cybercriminal and it is incumbent on prosecution to prove his case beyond a reasonable doubt; unfortunately, this is not the case because there is a scarcity of savvy prosecutors in the country.

Cybercriminals, on the other hand, have unrestricted access to renowned private prosecutors that demand exorbitant defense rates, which is not a challenge for them since they can easily afford to pay large professional fees to the finest cybercrime lawyers. Furthermore, the anonymity issue of cybercriminals, as well as the nature of evidence, which is often shaky due to the fact that investigators can only rely on traces and tracks left on computers and the Internet, all add to the case of prosecutors who are not as well-versed in handling cybercrime litigation as their private practice counterparts; these identified gaps are unfortunate.

4.7LET'S SUM UP

In this chapter, we have learned various challenges to enforcement of cybercrime. We have also worked on multiple concepts surrounding cybercrime. Besides, we analysed the position in USA and its similarity with Indian context.

[38] Paganini P (2013). InfoSec Institute 2013 Cost of cybercrimes http://resources.infosecinstitute.com/cybercrime-and-theunderground-market/

4.8FURTHER READING

- Ahamad M, Amster D, Barrett M, Cross T, Heron G, Jackson D, King J, Lee W, Naraine R, Ollmann G, Ramsey J, Schmidt HA, Traynor P (2008). Emerging Cyber Threats Report for 2009, Georgia Tech Information Security Centre. Georgia Inst. Technol. 9p.
- Ajayi EFG (2015). The Challenges to Enforcement of Cybercrimes Laws and Policy. International Journal of Information Security and Cybercrime, 4(2):33-48. Available at: http://www.ijisc.com/year-2015- issue-2-article-4/ Ajayi EFG (2016). The Impact of Cybercrimes on Global Trade and Commerce.
- Bassiouni MC (1999). The Sources and Content of International Criminal Law: A Theoretical Framework, 1 International Criminal Law 3-126. 2:353-356
- Centre for Strategic and International Studies (CSIS) (2014). Net Losses - Estimating the global cost of cybercrime. Economic impact of cybercrime II. June 2014. pp. 1-24. Available at: http://www.mcafee.com/us/resources/reports/rp-economic-impactcybercrime2.pdf Chang W, Chung W, Chen H, Chou S (2003).
- An International Perspective on Fighting Cybercrime, ISI'03 Proceedings of the 1st NSF/NIJ conference on Intelligence and security informatics. pp. 379-384.
- Commonwealth, Litigation Practice (1962). Macfoy versus United Africa Company Limited (West Africa). PC 27 NOV 1961.

4.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is Extradition?

The term extradition is made up of two French words: ex, which means “out,” and custom, which means “deliverance.” That is the method of a new judicial jurisdiction recalling someone convicted of a crime for conviction or punishment. Extradition is often known as the transfer of an individual convicted of committing an offense in one country to another.

2. Define Cybercrime

Every criminal or other offence facilitated or involving the use of electronic messages or computer systems, including any software or the Internet, or any more or more of them, is referred to as cybercrime.

4.10 ACTIVITY

Elaborate specific reasons for challenges in enforcement of cybercrime. (Word count- 2000 to 2500 words)

Block-2

ARTIFICIAL INTELLIGENCE AND CYBER LAW

Unit 1: THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

1

Unit Structure

1.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- The relationship between Artificial intelligence and Cyber security
- Concept of machine learning.
- Detailed analysis of cyber security.

1.2 INTRODUCTION

In the modern age, cyber defense has become a big concern. Data hacks, identity fraud, captcha breaking, and other such reports abound, involving millions of people as well as businesses. The challenges have always been endless in terms of devising appropriate controls and protocols and putting them in place with pinpoint accuracy in order to combat cyber threats and crimes. With recent advances in artificial intelligence, the possibility of cyber threats and crimes has increased exponentially. It has been used in almost every scientific and engineering area. AI has revolutionized everything from hospitals to robots. Since cyber criminals couldn't keep this ball of fire from them, "normal" cyber attacks have evolved into "intelligent" cyber attacks.[39]

"Intelligence" is only one of the characteristics that separates humans from all creatures on the globe. While machines cannot have that inherited intellect, the thought of getting that intelligence in man-made machines is intriguing. Instead of normal human intellect, scientists, philosophers, and those working to explain the human mind began to wonder, "Why can't robots think?" The concept of developing "Artificial Intelligence" started to draw the interest of scholars all over the world as a result of multidisciplinary activities in brain science, neuroscience, and computer science.

Researchers began to have high hopes for AI science in the 1960s and 1970s, but they were mostly disappointed because no breakthroughs were made. Artificial intelligence can be described as a scientific area that attempts to understand and model human intelligence. Many researchers have their own interpretations of AI, citing Artificial Intelligence: A Modern Perspective by Peter Norvig and Stuart Russell

[39] Bhatele, Kirti Raj &Shrivastava, Harsh. (2019). The Role of Artificial Intelligence in Cyber Security. 10.4018/978-1-5225-8241-0.ch009.

as an example.[40] "The analysis of agents that live in the world and understand and behave is known as Artificial Intelligence." For decades, there has been a push to develop technologies that can perceive, think, read, and act like humans.

1.3HISTORICAL ATTEMPTS

For the first time in 1943, Warren McCulloch and Walter Pitts tried to construct an intelligent device. They suggested a model of an artificial networked neural system, claiming that if properly defined, it might learn in the same way as the human brain. Alan Turing wrote "Computer Machinery and Intelligence" a year ago, in which he discussed the concept of "Artificial Intelligence."[41] He also suggested the "Turing test" as a way to calculate a machine's ability to exhibit intellect in his work. The examination involves a computer that generates natural language, an evaluator (who is human), and a human. The evaluator can converse (interact) with both the computer and the person in order to classify the machine. Both the computer and the human will attempt to convince the evaluator that they are conversing with another human. If the evaluator is unable to differentiate between computer and human conversation, the machine would be deemed intelligent.

In 1956, John McCarthy invented the word "Artificial Intelligence." He developed LISP, a high-level AI programming language for use in AI applications, two years later. We'll go over one of the most commonly used AI approaches in the next section, and then we'll go over the latest and strongest AI approach (Pattern Recognition).

Artificial Intelligence has the potential to provide large incremental value to a wide range of sectors globally, and is expected to be the key source of competitive advantage for firms.

a) Healthcare: Application of AI in healthcare can help address issues of high barriers to access to healthcare facilities, particularly in rural areas that suffer from poor connectivity and limited supply of healthcare professionals. This can be achieved through implementation of use cases such as AI driven

[40] Bai, J., Wu, Y., Wang, G., Yang, S. X., &Qiu, W. (2006). A very distinctive intrusion detection model based on multilayer self-organizing maps and principal part analysis. In Advances in Neural Networks. Springer.

[41] Chatzigiannakis, V., Androulidakis, G., &Maglaris, B. (2004). A Distributed Intrusion Detection Prototype Using Security Agents. In Proceedings of Workshop of the HP Open View University Association. University of Evry.

diagnostics, personalised treatment, early identification of potential pandemics, and imaging diagnostics, among others.

b) Agriculture: AI holds the promise of driving a food revolution and meeting the increased demand for food (global need to produce 50% more food and cater to an additional 2 billion people by 2050 as compared to today). It also has the potential to address challenges such as inadequate demand prediction, lack of assured irrigation, and overuse / misuse of pesticides and fertilisers. Some use cases include improvement in crop yield through real time advisory, advanced detection of pest attacks, and prediction of crop prices to inform sowing practices.

c) Smart Mobility, including Transports and Logistics: Potential use cases in this domain include autonomous fleets for ride sharing, semi-autonomous features such as driver assist, and predictive engine monitoring and maintenance. Other areas that AI can impact include autonomous trucking and delivery, and improved traffic management.

d) Retail: The retail sector has been one of the early adopters of AI solutions, with applications such as improving user experience by providing personalised suggestions, preference-based browsing and image-based product search. Other use cases include customer demand anticipation, improved inventory management, and efficient delivery management.

e) Manufacturing: Manufacturing industry is expected to be one of the biggest beneficiaries of AI based solutions, thus enabling 'Factory of the Future' through flexible and adaptable technical systems to automate processes and machinery to respond to unfamiliar or unexpected situations by making smart decisions. Impact areas include engineering (AI for R&D efforts), supply chain management (demand forecasting), production (AI can achieve cost reduction and increase efficiency), maintenance (predictive maintenance and increased asset utilisation), quality assurance (e.g. vision systems with machine learning algorithms to identify defects and deviations in product features), and in-plant logistics and warehousing.

f) Energy: Potential use cases in the energy sector include energy system modelling and forecasting to decrease unpredictability and increase efficiency in power balancing and usage. In renewable energy systems, AI can enable storage of energy through intelligent grids enabled by smart meters, and also improve the reliability and affordability of photovoltaic energy. Similar to the manufacturing sector, AI may also be deployed for predictive maintenance of grid infrastructure.

g) Smart Cities: Integration of AI in newly developed smart cities and infrastructure could also help meet the demands of a rapidly urbanising population and providing them with enhanced quality of life. Potential use cases include traffic control to reduce congestion and enhanced security through improved crowd management.

h) Education and Skilling: AI can potentially solve for quality and access issues observed in the Indian education sector. Potential use cases include augmenting and enhancing the learning experience through personalised learning, automating and expediting administrative tasks, and predicting the need for student intervention to reduce dropouts or recommend vocational training.[42]

1.4KNOWLEDGE OR RULE-BASED APPROACH

We aim to embed the expertise of human experts for decision-making in Knowledge-based AI systems. The aim is to give the machine the information it needs to perform a mission, such as medical diagnosis, as well as the guidelines it needs to infer ideas from that knowledge and make a decision.[43] All of the decisions made by the KBAI algorithm would be influenced solely by the knowledge base provided by a human expert in the field. As a result, KBAI systems are often referred to as Expert Systems. As a result, the KBAI system's general architecture consists of a Knowledgebase and an Inference Engine. For inference from the knowledge base, most inference engines use IF-EISE laws. MYCIN was the first knowledge-based method. It was created for the purpose of medical diagnosis. The fundamental idea behind information-based structures was to specifically interpret knowledge using IF-EISE laws (Russell, S., J., &Norvig, P., 2000). The role of designing an AI system

[42] http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf

[43] Bostrom, N. (2015), TED Talk on Artificial Intelligence. Retrieved from https:// en.tiny.ted.com/talks/nick_bostrom_what_happens_when_our_computers_get_ smarter_than_we_are

revolves around the representation of information. The rule-based information representation was heavily used in IBM Watson's production.[44]

1.5PATTERN RECOGNITION

Another path to Artificial Intelligence is pattern analysis. In contrast to the rule-driven approach, it is based on results. It tries to derive information from the results. To discover patterns from the data, we just need data and a machine learning algorithm (section 2). These patterns can be used to derive the system's decisions in an uncertain world. The following is a modern example of pattern identification (according to Bishop): The field of pattern recognition is concerned with the automated detection of regularities in data using computer algorithms, as well as the use of these regularities to perform activities such as data classification. The best approach to Artificial Intelligence has been pattern detection. When it comes to pattern recognition, machine learning is the most effective method. We'll go into it in detail in the next segment (Russell, S., J., &Norvig, P., 2000).

1.6MACHINE LEARNING

The last innovation that mankind will ever need is machine intelligence (Bostrom, N., 2015) Arthur Samuel invented the term "machine learning" in 1959. "Machine learning is the area of research that enables the robot to learn without being directly programmed," he says. This concisely expresses the central concept. Unlike previous methods that attempted to specify a large number of laws in order to gain information from data, machine learning creates systems that learn certain rules from the data themselves. This method is more akin to normal learning.[45]

A child, for example, learns to recognize an apple after being given several examples of apples. Similarly, we provide a large amount of data to the computer, and the machine develops an understanding for the data on its own. "A computer program is said to benefit from experience E with respect to any class of tasks T and output measure P if its performance at tasks in T, as measured by P, increases with experience E," according to Tom Mitchell. The Machine learning algorithm refers to

[44] Iftikhar, B., &Alghamdi, A. S. (2009). Application of artificial neural network within the detection of dos attacks. Proceedings of the ordinal international conference on Security of knowledge and networks, 229–234.

[45] Kivimaa, J., Ojamaa, A., &Tyugu, E. (2008). Pareto-Optimal state of affairs Analysis for the selection of Security Measures. Proceedings of Military communications conference, MILCOM 2008.

the algorithms that enable machines to learn. In general, there are two types of machine learning algorithms: supervised learning and unsupervised learning (Russell, S., J., &Norvig, P., 2000). Other types of machine learning include reinforcement learning and others.

1.7SUPERVISED MACHINE

Educating yourself the data is named in supervised learning. Let's assume we want the machine to be able to tell the difference between photographs of cats and other images. We'll write a program that takes an image as input and determines whether or not it's a cat (i.e. 1 for cat and 0 for non-cat). We must first train the computer in order to complete this mission. This means that for a huge number of photographs, we'll first show the computer that this is a cat image, this is a noncat image, and so on.[46] Then we'll assess how well it does on pictures it has never seen before. If the performance falls short of our expectations, we will retrain it with more details. The data used for preparation is referred to as the "training package," while the data used to assess the learned structure or "Model" is referred to as the "testing set." The term "Sample" refers to data examples of photographs. In the supervised learning setup, each sample has a matching true mark. The topic we discussed is referred to as "Classification," because there are only two classes: cat and non-cat.

It's called "Binary Classification" where there are just two classes, and "Multi-class classification problem" when there are more than two classes. In contrast to the classification issue, we want our regression method to forecast "continuous values." Predicting house prices in a neighborhood, for example. What information do we need to gather in this scenario? We'll try to gather information on the factors that influence house prices, such as house size, number of rooms, and so on. In machine learning language, the parameters are referred to as "Features." We'll also include real sample prices in the training set, but not in the evaluation set (obviously, this is the data we use to test our system). Another example of regression is forecasting stock exchange values. Another classification example may be used to determine

[46] Jonze, S. (2017). 28 Best Quotes About Artificial Intelligence. Retrieved from https:// www.forbes.com/sites/bernardmarr/2017/07/25/28-best-quotes-about-artificialintelligence

whether or not an individual has cancer.[47] You came up with the concept (Russell, S., J., &Norvig, P., 2000).

1.8UNSUPERVISED LEARNING

We don't have the sample's true mark or meaning in unsupervised learning. The information is not classified. The unsupervised learning algorithm's goal is to discover structure in the input data. Its aim is to uncover secret trends in data. It attempts to organize the data into distinct categories based on their characteristics (Russell, S., J., &Norvig, P., 2000). Clustering is the term for this mission. Let's take a look at how this is beneficial. A publishing house wishes to increase its revenues. It has a vast array of information on its consumers' purchasing habits. The company feeds the data into a "Cluster" learning algorithm, which produces 5 consumer segments, and the company discovers that the first segment enjoys romantic genre books, the second enjoys x genre books, and so on. With this knowledge, the organization will tailor its offering to specific business segments. Clustering methods have been used in astronomy, computer science, and other fields.

1.9CYBER SECURITY

Consider a package, for example (Artificial Intelligence, Machine Learning, Block Chain, Deep Learning, Big Data Analysis, Data Science, Internet of Things etc.). This collection includes some of today's most exciting and talked-about developments. In this period of rapidly growing Internet growth and intense workloads in the fields mentioned above, cyber-security has become a major concern.

The word "cyber" refers to "computer culture, information media, or/and virtual reality." This makes it clear that we're about machine, network, and information security. To clarify, cyber security refers to the different measures/techniques used to secure integrated networks, applications, hardware, and data from cyber-attacks (unauthorized access and damage).Where it comes to computers, both cyberspace and physical space security are equally essential. Cyber security includes

[47] Kivimaa, J., Ojamaa, A., &Tyugu, E. (2009). Graded Security accomplished System. In Lecture Notes in engineering (Vol. 5508, pp. 279–286). Springer.

components such as application security, information security, network security, organizational security, and others that function together to secure the whole information infrastructure. This architecture resembles a multilayer security scheme that is distributed across the system and involves different system components, and it is one of the most effective defensive mechanisms possible.[48]

1.10ROLE OF CYBERSECURITY

Thanks to the evolving existence of cyber-risks, the general public is becoming more vulnerable to cyber-attacks. Pathways are built by malicious and aggressive practices that grant predators (hackers and crackers) unwanted access to computer systems or networks. Cyber attacks are the term for these types of operations. To create these paths, predators focus on the system's or network's glitches and flaws. Ransomware, malware, worms, Trojans, spyware/adware, attack vectors, social engineering, Man in the Middle (MITM), and other cyber threats abound (Panimalar, A., Giri, P.U. & Khan, S., 2018).[49]Everyone has important assets and sensitive data under their control, and when an individual gains access to those assets and data, they may do significant harm. In the case of cyberspace, these unauthorized accesses may be the product of one or more cyber attacks. Here's where cybersecurity falls through. It ensures your system's or network's functionality, confidentiality, and honesty, as well as its performance, without jeopardizing protection.

1.11 PRINCIPLES OF CYBER SECURITY (PRINCIPLES FORMING THE BASE FOR CYBERSECURITY)

Any basic yet useful guidelines should be adopted to ensure the three essential priorities of cyber security, namely availability, confidentiality, and integrity.[50]

1. Prioritize Prior Devices: Stabilizing the degree of availability, anonymity, and dignity of services is one of the most difficult tasks, and it is accomplished by concentrating on the most important systems and ensuring the highest security cover for them, whereas other approaches are used to secure less important systems.

[48] Kurzweil, R. (2005). The Singularity is near. Penguin Group.

[49] Russell, S. J., &Norvig, P. (2000). Artificial Intelligence: A Modern Approach. Prentice Hall.

[50] Preda, M. D., Christodorescu, M., Jha, S., &Debray, S. (2008). A Semantics-Based Approach to Malware Detection. ACM Transactions on Programming Languages and Systems, 30(5), 1–54. doi:10.1145/1387673.1387674

2. Different Users, Different Levels of Accessibility: Who has access to what data can be determined by the class of user, and no one person can have complete access to all data and knowledge. This ensures that a specific duty has the bare minimum of rights. As a result, changes in rights are proportional to changes in obligation.[51]

3. Independent Protection (Protocols): Using multiple authentication protocols for a single job is much easier than using only one. It greatly decreases the probability of effective cyber-attacks, and the basic idea is to make the perpetrator work harder by requiring him to perform several actions in order to get through several layers of defenses.

4. Backups: Failures can happen, but preparing for the repercussions can help minimize the severity of the damage to the system, network, or person. This is a particularly versatile technique that is used in a variety of areas.

Keeping track of all breaches: Cyber security personnel should keep track of all breaches, which should be studied and safety mechanisms developed on a regular basis. Since hackers aren't waiting, this phase can move quickly. They're honing their talents and refining their cyber-attack tools (Panimalar, A., Giri, P.U. & Khan, S., 2018).

1.12 LET'S SUM UP

We studied basic artificial intelligence strategies that are promising in this chapter. It looked at how such methods could be used in cyber defense. We have spoke about the future of artificial intelligence and cyber defense.

1.13FURTHER READING

- Lunt, T. F., &Jagannathan, R. (1988). An example amount of your time Intrusion Detection accomplished System. Proceedings of IEEE conference on Security and Privacy.
- Nappo, S. (2017). Goodreads. Retrieved from https://www.goodreads.com Panimalar, A., Giri, P.U. & Khan, S. (2018). Artificial Intelligence Techniques

[51] Yu, W., Zhang, N., Fu, X., & Zhao, W. (2010). Self-Disciplinary Worms and Countermeasures: Modeling and Analysis. IEEE Transactions on Parallel and Distributed Systems, 21(10), 1501–1514. doi:10.1109/TPDS.2009.161

in Cyber Security. International Research Journal of Engineering and Technology, 5(3).

- Preda, M. D., Christodorescu, M., Jha, S., &Debray, S. (2008). A Semantics-Based Approach to Malware Detection. ACM Transactions on Programming Languages and Systems, 30(5), 1–54. doi:10.1145/1387673.1387674
- Russell, S. J., &Norvig, P. (2000). Artificial Intelligence: A Modern Approach. Prentice Hall. Salvador, P., Nogueira, A., França, U., &Valadas, R. (2009).
- Framework for Zombie Detection Using Neural Networks. Proceedings of The Fourth International Conference on Internet Monitoring and Protection ICIMP. 10.1109/ICIMP.2009.10

1.14CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is machine learning?**

“Machine learning is a branch of computer science that enables a computer to learn without being directly programmed.” This concisely expresses the central concept. Unlike previous methods that attempted to specify a large number of laws in order to gain information from data, machine learning creates systems that learn certain rules from the data themselves.

2. **What is cyber security?**

Cyber security refers to a collection of steps and strategies for defending interconnected networks, applications, hardware, and data from cyber-attacks (unauthorized access and damage). Where it comes to computers, both cyberspace and physical space security are equally essential. Cyber security includes components such as application security, information security, network security, organizational security, and others that function together to secure the whole information infrastructure.

1.15 ACTIVITY

Explain machine learning and types of supervisions under artificial intelligence. (Word count 2000 to 2500)

Unit 2: ARTIFICIAL INTELLIGENCE AND CYBER SECURITY: OPPORTUNITIES AND CHALLENGES

2

Unit Structure

2.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- About human-Artificial Intelligence interactions
- AI decision making and its detection

2.2 INTRODUCTION

Recent Artificial Intelligence (AI) breakthroughs are game-changing, and they still outperform humans in tasks like visual detection, natural language processing, and data analytics. Economic dynamics will accelerate the introduction of new AI technologies that will disrupt nearly every area of business, both positively and negatively. Artificial intelligence technologies can be abused, evaded, and misled, posing serious security risks for devices such as network management software, financial systems, and self-driving cars. As a result, strategies and best practices that are safe and resilient are critical.[52]

Just as AI programs need novel cyber security techniques and approaches to enhance their trustworthiness and resiliency, cyber security will benefit from AI by increasing understanding, responding in real time, and improving overall effectiveness. This involves self-adaptation and modification in the face of continuing threats that change the existing attacker-defender imbalances. Strategies that use AI to categorize different types of attacks and notify adaptive solutions (e.g., spot anomalies easily and know how to repair them) at scale can use AI to recognise an adversary's vulnerabilities, use observation techniques, and gather lessons learned. It is well known that a small group of skilled cyber defenders can successfully secure networks that are used by tens of thousands of people. AI could apply the same degree of device security, making it universal and providing the domain information required to solve issues like quality-of-service restrictions and system failure behaviors.

[52] Cloud adoption risk report 2019 (pdf). https://mscdss.ds.unipi.gr/wp-content/uploads/2018/10/Cloud-Adoption-Risk-Report-2019.pdf (2019).

2.3HUMAN-AI INTERFACES

As threats become more complicated and serious, collaboration between AI-based cyber security systems becomes more relevant, as does coordination and trust between human-AI interfaces. Specific system elements optimize their own targets without considering system-level priorities, which causes challenges with everything from business IT to self-driving vehicles.[53] Attackers can make a module behave in a way that is ideal locally but pathological globally. Furthermore, in an age where facts can be misinterpreted, misattributed, or distorted, effective decision-making necessitates hybrid methods that combine and orchestrate human and AI capacities and viewpoints.[54]Three relevant research areas to include human-machine collaboration, fostering trust in systems and people, and delivering decision-making assistance. Human-machine collaboration must be structured in such a way that humans can comprehend, trust, and explain the results. Users must be taught how to have priorities, input, and well-formatted and meaningful data, as well as how to understand their role in the decision-making process. Human integration research is required to optimize results while minimizing latency and negative effects. To give time for human decision-making, AI is often used to automatically shut down suspicious activity.

Will this also be the case when AI is introduced to vital infrastructure like the electrical power grid, where even a brief outage could be exceedingly widespread, destructive, or dangerous? Slowing AI mechanisms to handle humans in the loop is one solution. While this would limit mobility, it would empower humans to interfere and repair failed parts. Interactions between humans and AI systems must be handled with the intention of reducing human error, increasing protection, and providing oversight in a complex human-AI system world. Adopters and users of AI systems must consider and trust the system's function.[55]

Humans must be able to recognize a system's state and forecast its behaviour under different conditions in order to have the appropriate degree of confidence.

[53] Ai in cyber security-capgemini worldwide. https://www.capgemini.com/news/ai-in-cyber security/ (2020).
[54] Ai index 2019 report (pdf). https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf(2020).
[55] Congnigo-infosecurity magazine. https://www.infosecurity-magazine.com/directory/cognigo/ (2019).

Overtrust can lead to a refusal to override a misbehaving system, while undertrust can lead to the abandonment of a system that is otherwise reliable. Human-readable, rule-based requirements based on approximating device behaviour, as well as consideration of cognitive and other biases, are needed for determining the appropriate degree of confidence. AI systems can produce incredibly persuasive false video and audio that humans can believe, according to research. Decision-making aid, such as teaching human operators to survive data falsification attacks, and AI-models that can anticipate failure modes and adjust as humans make incorrect decisions, must be included in research.

2.4TRUSTWORTHY AI DECISION MAKING

When AI systems are implemented in high-value environments, it's critical to ensure that the decision-making mechanism is reliable, particularly in adversarial scenarios. Although there are various examples of ML flaws, science-based methods for predicting trustworthiness remain elusive. Methods and concepts for a broad range of AI programs, including machine learning, planning, inference, and information representation, need research. Defining success indicators, designing methods, keeping AI programs explainable and accountable, strengthening domain-specific teaching and thinking, and handling training data are all areas that need to be discussed for trustworthy decision making.[56]To integrate robustness, anonymity, and fairness into decision-making algorithms, threat model research must recognise observable properties that determine trustworthiness.

To attain these trustworthiness properties, the device would have to reason about adversarial intervention and identify requisite criteria based on a particular threat model. Adapting cryptography or computer security concepts, unifying properties into a single logic system, and considering them as variations of a single notion of (in)stability in ML and AI for both decision making and security models more generally are both possibilities. Methods for understanding the learned reasoning of AI methods, especially deep learning, are also in need of research. What impact do those data points have on the optimization and reasoning procedures used in

[56] Knowledge-directed artificial intelligence reasoning over schemas (kairos). https://www.darpa.mil/program/knowledge-directed-artificial-intelligence-reasoning-over-schemas (2020).

machine learning systems? Analysis of the optimization process or the AI system effect, whether it captures both the training data and the learning form, are both possibilities. Techniques for estimating the effect of a training point on individual predictions may be used to determine a model's validity in a decision context. In machine learning, there are new methods that use a range of strategies to include decision assurances (e.g., convex relaxation of the adversarial optimization problem and randomized smoothing).

However, the techniques are almost entirely based on supervised learning at the moment, which is difficult to do without compromising machine efficiency. AI systems that require advice when they are unsure, a related field of study, will increase confidence in the final decision and help the system to gain knowledge for future decision making. AI's precision is also domain-specific. When training data is not indicative of the specified context, security vulnerabilities occur. In contrast, if application domain restrictions are not taken into account, excessively pessimistic risk tests will occur. Within domain-specific AI ecosystems, as well as as they become a part of the full-use ecosystem, further research is required on how input data is acquired, secured, preserved, and evaluated. An autonomous vehicle system is trained with photographs and circumstances gathered from real-world scenarios and is kept up to date as its surroundings alter. Domain-specific vulnerabilities must be recognized in perception, planning, reinforcement learning, information representation, and reasoning.

2.5DETECTION AND MITIGATION OF ADVERSARIAL INPUTS

Though AI excels at many tasks, it is susceptible to erroneous inputs that cause learning, reasoning, and planning processes to yield incorrect results. Limited quantities of feedback noise crafted by an opponent have been shown to fool deep learning methods in the past. As a result of these technologies, adversaries can monitor networks without fear of being detected.[57]If deep learning and other machine learning and AI algorithms becoming more embedded into operating

[57]Darpa robotics challenge (DRC) using human-machine teamwork to perform disasterresponse with a humanoid robot. https://apps.dtic.mil/docs/citations/AD1027886 (2020).

frameworks, it is important to consider more rigorous machine learning approaches, AI reconnaissance prevention, the analysis of adversarial models, model poisoning prevention, safe testing protocols, data protection, and model fairness to protect against adversarial inputs. Efforts to harden learning methods against adversarial inputs are needed. Both the statistical and technical community are aware of the problem. To make the same advancements in deep learning and modern ML methods without losing efficiency or precision, both theoretical and empirical research is needed.

Modern AI systems are vulnerable to reconnaissance attacks, in which adversaries challenge the systems and learn about the internal decision reasoning, information bases, and training data. This is often a precursor to an attack aimed at extracting security-relevant training data and references or obtaining the AI's intellectual property.[58] The following are some potential reconnaissance mitigation steps that should be investigated further:

- By inverting the model, you will increase the attacker's workload while lowering their efficacy.
- Use encryption techniques such as rate restricting, access controls, and deception.
- Study the effects of algorithms and processes on precision and other factors.
- Create algorithms and methods that are vulnerable to reconnaissance.
- Incorporate opposition into optimizations for learning and reasoning.
- Using modern multistep methods, embed security protections into the model.
- Using the cyber security honeypot4 model, reveal the attacker's existence and objectives. The adversary's expertise and skills identify an AI system's weakness.

To identify the various types of attacks and build effective defenses, further research is needed. Attacks must be addressed according to the kind of information that the perpetrator has access to. These models should be carefully mapped,

[58] Aljurayban NS, Emam A (2015) Framework for cloud intrusion detection system service. In: 2015 2nd world symposium on web applications and networking (WSWAN), pp 1–5

attack and protection tactics should be established, and particular research attention should be paid to security-critical environments where ML models are most vulnerable. (For example, self-driving cars and malware detection).

From training results, AI and machine learning models learn how to classify predicted inputs. The model outputs would be inconsistent if the training instances do not reflect both possible and potential scenarios. As a result, an attacker will manipulate the model and implement a loophole that can be exploited. And if an opponent only controls a portion of the training sample, the model's behaviour may be influenced (model poisoning). ML needs as much data as possible, and using multiple data sources is popular, but dangerous. The entire paradigm becomes untrustworthy if any one source of data is malicious.[59]AI best practices must guarantee the end-to-end provenance of training data and the identification of data that comes beyond the usual input space to help prevent adversarial poisoning and enhance training processes.

When used on identical data to what they were educated on, machine learning techniques perform well, but when the data is new, they struggle (e.g., a self-driving car trained in sunny, cloudy, rainy, and snowy weather might operate poorly in sleet or hail). There are general issues since gathering data for all potential scenarios is difficult. And where a person does, systems normally do not detect suspicious data. The aim of the study is to improve anomaly identification, implement training methods that intensify unusual events, and make the best use of existing training data and algorithms.ML models must be retrained on a regular basis to stay successful and reliable (e.g., social media terminology used for public sentiment analysis changes over time as vocabulary and topics of interest change). To determine what training data to obtain, when such training data is no longer valid, and how much models should be retrained, further research is needed. An adversary can decide if a data item was used in training a model, according to recent attacks. Many applications necessitate ML training for private data, putting personal data at risk.

More research is required, but advancements like differential privacy open up new

[59]Bao H, He H, Liu Z, Liu Z (2019) Research on information security situation awareness system based on big data and artificial intelligence technology. In: 2019 international conference on robots intelligent system (ICRIS), pp 318–322

avenues for anonymizing data and preventing leaks. Finally, models can pick up on any prejudices and biased characteristics in the training results. If the evidence shows prejudice towards a certain population (for example, in college enrollment or loan approvals), the result would show that bias. The development of scientific and technological foundations for ML justice would be needed to prevent outcome bias. To quantify, identify, and diagnose unequal ML training data and procedures, goals must be established and algorithmic techniques built.

2.6 LET'S SUM UP

We studied basic artificial intelligence techniques and the principle of machine learning in this chapter. We have also figured out how humans and AI communicate and how it affects cyber rules.

2.7FURTHER READING

- Johnson, J. (2014). Remarks by Secretary of Homeland Security Jeh Johnson at the White House Cyber security Framework Event. Retrieved from https://www.dhs.gov/news/2014/02/12/remarks-secretary-homeland-security-jeh-johnson-white-house-cyber security-framework
- Jonze, S. (2017). 28 Best Quotes about Artificial Intelligence. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/07/25/28-best-quotes-about-artificial-intelligence
- Kivimaa, J., Ojamaa, A., &Tyugu, E. (2008). Pareto-Optimal state of affairs Analysis for the selection of Security Measures. Proceedings of Military communications conference, MILCOM 2008.
- Kivimaa, J., Ojamaa, A., &Tyugu, E. (2009). Graded Security accomplished System. In Lecture Notes in engineering (Vol. 5508, pp. 279–286). Springer.
- Kurzweil, R. (2005). The Singularity is near. Penguin Group.

2.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

What is cyber security?

Cyber security refers to a collection of steps and strategies for defending interconnected networks, applications, hardware, and data from cyber-attacks (unauthorized access and damage). Where it comes to computers, both cyberspace and physical space security are equally essential. Cyber security includes components such as application security, information security, network security, organizational security, and others that function together to secure the whole information infrastructure.

How does cyber security benefit from AI?

Just as AI programs need novel cyber security techniques and approaches to enhance their trustworthiness and resiliency, cyber security will benefit from AI by increasing understanding, responding in real time, and improving overall effectiveness. This involves self-adaptation and modification in the face of continuing threats that change the existing attacker-defender imbalances. Strategies that use AI to categorize different types of attacks and notify adaptive solutions (e.g., spot anomalies easily and know how to repair them) at scale can use AI to recognise an adversary's vulnerabilities, use observation techniques, and gather lessons learned. It is well known that a small group of skilled cyber defenders can successfully secure networks that are used by tens of thousands of people.

2.9 ACTIVITY

Explain AI decision-making process and AI- human interaction. (Word count 2000 to 2500)

Unit 3: ARTIFICIAL INTELLIGENCE POLICY IN INDIA: A FRAMEWORK FOR ENGAGING THE LIMITS OF DATA-DRIVEN DECISION-MAKING

3

Unit Structure

3.1 LEARNING OBJECTIVE

In this chapter, we will learn-

- Policy making for Artificial intelligence
- AI related concepts like machine learning and process involved in AI decision-making.
- NITI aayog strategy for Artificial intelligence.

3.2 INTRODUCTION

The word Artificial Intelligence (AI) remains in vogue more than half a century since it was coined. Artificial intelligence determines the content we consume on social media, determines risk judgments of offenders in criminal sentencing, determines credit-worthiness of people, and also suggests the best path home from work. Most AI systems are trained on historical data and are capable of detecting trends, learning from examples, and forecasting potential outcomes for decision-making purposes. This generalizations are focused on massive databases that humans will be unable to interpret at the same speed and size.[60]AI's effect is thought to be so revolutionary that it has been dubbed the "new electricity." The social and ethical ramifications of these innovations have come into view as industry and policymakers work to evolve and apply them.

Since the Indian government places a high priority on new technology in the digital economy, AI strategy will change and grow quickly in the coming years. Aadhaar, the world's largest biometric identification initiative, is located in the country and, depending on how it is used, will serve as a focal point for AI applications. India is also at a crucial juncture in the implementation of data security legislation, which will have a significant impact on how AI can and can work in the country.

Although the introduction addresses the issue that this article aims to solve, the next section will go over the chapter's intended scope and include definitions and

[60]Balkin J. 2017 Free speech in the algorithmic society: big data, private governance, and new school speech regulation. U.C. Davis L. Review, Forthcoming 2018. See https://papers.ssrn.com/sol3/paperscfm?abstract_id=3038939.

logical clarifications for technical terms used in the chapter.[61] It will address the current state of India's AI policy environment before taking the reader through each stage of the framework, with the aim of providing theoretical history for thinking through the proposed framework. Finally, this approach is applied to industries that are actually being discussed by India's policymakers. Conclusions and reflections will be used at the end of the chapter.[62]

3.3SCOPE

The word "AI" can be interpreted in a variety of ways. Given the difficulty in defining terminology in this field, I explain a few technical terms in this section and describe their intended reach within the context of this article. - A collection of "encoded procedures for converting input data into desired results, based on precise formulas" is referred to as an algorithm. It's a methodical, step-by-step process that doesn't rely on human instincts or guesswork.[63]

Artificial intelligence refers to a computer's ability to behave intelligently. There are three forms of AI. The first is artificial superintelligence, which is the concept that machines can outperform humans in terms of intelligence, social abilities, and scientific expertise in a variety of realms. Artificial general intelligence is the second. This applies to the target of machines displaying knowledge in many contexts, if not on par with human intelligence. Any of these AI types are both technically conceivable and completely implausible, according to some researchers.The third kind is artificial narrow intelligence (ANI), which refers to computers' ability to mimic human skills in specific, intentional domains. The word AI will be used to refer to ANI alone for the purposes of this paper.

Machine learning (ML) is the most effective and widely used branch of AI strategies today, demonstrating a system's ability to increase task efficiency over time. Today, much of what is referred to as "AI" is simply machine learning. Machine learning algorithms, according to Arthur Samuel, have the ability to learn without being directly coded. In order to increase efficiency on future assignments, machine

[61] Angwin J, Larson J, Mattu S, Kirchner L. 2016 Machine Bias. ProPublica. See https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[62] O'Neil C. 2016 Weapons of math destruction: how big data increases inequality and threatens democracy, pp. 278–315. New York, NY: Crown Publishing Group.

[63] O'Neil C. 2016 Weapons of math destruction: how big data increases inequality and threatens democracy, pp. 278–315. New York, NY: Crown Publishing Group.

learning relies on results. Existing research has demonstrated that data bias can result in overwhelmingly negative results, further entrenching societal prejudice.

The majority of machine learning applications rely on data. Developers of machine learning systems use training data to train variations of these algorithms. The paradigm evolves as a result of the preparation. Machine learning is an iterative technique, which entails a continuous process of analyzing these models and adapting training data and learning algorithms to optimize for performance, as described and decided by developers.

Machine-learning strategies, as previously said, depend for instructions on what to look for. Feature engineering, or choosing the characteristics the machine-learning algorithm can train, is an important human factor in machine learning.[64] In reality, this is a much more difficult job for developers than actually performing the learning process. Although attempts to minimize human interference in feature selection are growing, this is impossible.[65]

3.4 INDIA'S AI POLICY LANDSCAPE

The Indian government has placed AI growth, adoption, and promotion at the top of its priority list, based on the belief that AI has the ability to make people's lives simpler and society more equitable.[66] The Union government dedicated significant funds to research, training, and skilling in new technologies such as AI in 2018, an expansion of 100 percent over previous investments. This focus on emerging media is nothing new. The Digital India initiative of the Union government aims to turn India into a "digitally driven society and information economy."Digital India aspires to make digital technology a central utility for all people, integrating such digitisation into government, and eventually empowering citizens.

The Digital India initiative is responsible for increasing support for testing, training, and skilling in new technologies such as artificial intelligence. The government has also started working to ensure that AI technology is made in India and designed to benefit India, as part of its Make In India project, which aims to promote India as a

[64] Elish MC, Hwang T. 2016 An AI Pattern Language, Intelligence and Autonomy initiative (I&A) at Data & Society. See https://www.datasociety.net/pubs/ia/AI_Pattern_Language.pdf.

[65] Domingos P. 2012 A few useful things to know about machine learning. Commun. ACM 55, 78–87.

[66] Gillespie T. 2014 The relevance of algorithms, Media technologies: essays on communication, materiality and society 167.

global manufacturing hub. Though AI has been a major concern in emerging technology in general, a variety of AI-specific initiatives have also arisen.

3.5NITI AAYOG’S NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE: #AIFORALL

A government-run think tank, the National Institution for Transforming India (also known as NITI Aayog), has been charged with developing a national artificial intelligence strategy to guide the government’s AI efforts. In early May 2018, NITI Aayog partnered with Google to train and incubate startups looking to build and embed AI-based technologies into their business models in an attempt to improve economic productivity in India. In late May 2018, NITI Aayog and ABB India signed a letter of intent to ‘make core sectors of the Indian economy ready for a digitalized future and recognize the promise of AI, big data, and connectivity.’[67]

NITI Aayog’s ultimate target for a national AI strategy is to “leverage AI for economic growth, social change, and sustainable growth, and finally as a “Garage” for emerging and developed economies,” according to a discussion paper published in June 2018. The task of the NITI Aayog goes beyond simply proposing a policy approach; it also involves execution and deployment. In two aspects, the National Strategy goes beyond and above any other AI policy mechanism.[68] First, it admits that AI implementation has primarily been motivated by business interests to date, and it recognizes the “need to find a balance between limited financial effects concepts and the common good.”Second, it recognizes that AI implementations in different sectors should be accepted for their incremental benefit rather than their alleged transformational value.[69]

Among these positive changes in outlook, India’s national policy on AI’s practical advice and review leave a lot to be desired. Education, agriculture, healthcare, smart cities & infrastructure, and smart mobility & transportation are the five primary sectors where AI may have a positive social impact and require the government to

[67] NITI Aayog. 2018 National strategy for artificial intelligence. NitiAayog 46. See http:// www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AIDiscussion-Paper.pdf.

[68] Make ‘Artificial Intelligence’ work for India: PM. The Economic Times. See https://cio.economictimes.indiatimes.com/news/government-policy/make-artificial-intelligence-work-forindia-pm/62980259.

[69] Gupta K. 2018 NitiAayog partners with Google to grow India’s artificial intelligence ecosystem. Livemint. See https://www.livemint.com/Industry/fpnGnNQ8duTCRZOEpk 2P6M/Niti-Aayog-partners-with-Google-to-grow-Indias-artificial-i.html.

play a leading role, according to the study. The study advocates the use of AI for security purposes when addressing smart cities.AI devices that forecast crowd behaviour that can be used for crowd control, “sophisticated monitoring systems” that can monitor people’s activity and behavior, and social media intelligence networks that can help with public safety are among them.[70]

The report’s guidelines in the form of smart cities did not mention the major shortcomings of consistency and justice, as well as the negative effects of surveillance on fundamental rights. This is particularly concerning because India’s surveillance system currently lacks sufficient protections to protect against law enforcement agencies’ possible erosion of fundamental freedoms. As a result, AI-assisted monitoring should be the exception rather than the rule. The study acknowledges that bias is rooted in evidence, with the likelihood of such bias being compounded over time, when addressing justice in AI systems as an issue.

One potential solution is to “identify the in-built biases and determine their effect, and then find ways to reduce the bias,” according to the study. When the fact is that skewed evidence comes from a biased, unjust, unjust, and oppressive society, it takes a ceteris-paribus approach, i.e. all other factors are similar, merely defining and mitigating prejudice in datasets will expect to achieve fairer outcomes. This method has a flaw in that it only considers AI as a statistical construct, rather than as a socio-technical structure. Understanding and adapting to the social context in which these programs will operate is critical to reducing prejudice within them.Indeed, avoiding discriminatory consequences should be the aim. As Eubanks points out, unless automatic decision-making tools are designed to address socioeconomic inequities, their use would exacerbate them.[71]

3.6 LET’S SUM UP

Learned about the context of India’s existing AI policy environment, as well as the proposed roadmap for addressing India’s ongoing sectoral challenges. We learned about the possible dangers of data-driven decisions in general, and in the Indian context in particular, in order to influence current policy debates in the region.

[70] Sharma YS, Agarwal S. 2018 NitiAayog to come out with national policy on artificial intelligence soon. The Economic Times. See https://economictimes.indiatimes.com/news/ economy/policy/niti-aayog-to-come-out-with-national-policy-on-artificial-intelligencesoon/articleshow/63387764.cms.

[71] Artificial Intelligence Task Force. See https://www.aitf.org.in/.

3.7FURTHER READING

- Elish, M.C. 2016 Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction. We Robot 2016 Working Paper. (DOI: 10.2139/ssrn.2757236)India Stack. Available from http://indiastack.org/about/.
- Sainath, P. 2018 In India, Farmer's Face a Terrifying Crisis. The New York Times. Available from https://www.nytimes.com/2018/04/13/opinion/india-farmers-crisis.html.
- Eckerslet, P., & Cohn, C. 2018 Google Should Not Help the U.S. Military Build Unaccountable AI Systems. Electronic Frontier Foundation. Available from https://www.eff.org/deeplinks/2018/04/should-google-really-be-helping-us-military-build-aisystems.
- RakshaMantri Inaugurates Workshop on AI in National Security and Defence. Press Information Bureau, Government of India. Available from http://pib.nic.in/newsite/PrintRelease.aspx?relid=179445.

3.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is artificial intelligence?**

Artificial intelligence refers to a computer's ability to behave intelligently. There are three forms of AI. The first is artificial superintelligence, which is the concept that machines can outperform humans in terms of intelligence, social abilities, and scientific expertise in a variety of realms.

2. **What is machine learning?**

Machine learning (ML) is the most effective and widely used branch of AI strategies today, demonstrating a system's ability to increase task efficiency over time. Today, much of what is referred to as "AI" is simply machine learning. Machine learning algorithms, according to Arthur Samuel, have the ability to learn without being directly coded.

3.9 ACTIVITY

Explain NITI Ayog strategy for artificial intelligence. (Word count 2000 to 2500)

Unit 4: PROSPECTS OF ARTIFICIAL INTELLIGENCE IN TACKLING CYBER CRIMES

4

Unit Structure

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- What Artificial Intelligence is in a broader manner
- AI's role in the protection of cyber crimes
- How AI applications can defend cyber crimes

4.2 INTRODUCTION

Since we live in an interactive online environment, we now use the Internet for the majority of our daily interactions and commercial activities. Rising internet computing developments pose concerns about cyberspace information security. Threats and intrusions exist in cyberspace. People, companies, and governments are all targets of cyber-threats that travel at the speed of light. It is self-evident that the best way to defend against intelligent cyber devices is to use intelligent applications. Because of the high speed of cyber operation and the vast amount of data involved, cyberspace security cannot be done only by physical devices or human interaction.[72] To identify threats and make intelligent real-time decisions, it needs a significant amount of automation. It's difficult to create applications that efficiently protects against rapidly changing threats using traditional algorithms. This is why we need novel techniques, such as using Artificial Intelligence (AI) methods to help humans combat cybercrime by providing machines with versatility and learning capabilities.

4.3 CYBER CRIMES

Cybercrime is on the rise in tandem with the expansion of the Internet. Internet crime has multiple faces and is perpetrated in a variety of ways. The term "cybercrime" refers to criminal acts carried out using computers and the internet. Cybercrime is fueled by the evolution of the internet and its global diversity.[73] Cybercrime can be divided into two distinct groups. One of them considers the network to be a criminal object, such as interference, network system destruction, and so on. The rest are people who use the internet to commit crimes like theft.

While the term "cybercrime" has been widely used, it is difficult to describe precisely. "Cybercrime is a term used commonly to describe illegal activity in which computers or computer networks are a weapon, a target, or a location of criminal activity," according to Somaiya et al. (2014).[74] "Offenses perpetrated against individuals or groups of people with a criminal purpose to deliberately damage the victim's reputation or inflict physical or mental harm, or failure, to the victim directly or indirectly, using electronic telecommunication networks such as the Internet and cell

[72] Selma Dilek, HüseyinÇakır and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015

[73] Manveer Kaur, ShevetaVashisht, Kumar Saurabhi, "Adaptive Algorithm for Cyber Crime Detection", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (3), 4381 – 4384, 2012

[74] JheelSomaiya, DhavalSanghavi, ChetashriBhadane, "A Survey: Web based Cyber Crimes and Prevention Techniques", International Journal of Computer Applications (0975 – 8887), Volume 105, November 2014

phones," according to Halder et al (2011).Cybercrime, according to Kandpal et al (2013), "requires all unauthorized access to information and breaches of security such as anonymity, passwords, and so on through the use of the internet." Virus assaults, financial crimes, the selling of illegal articles, pornography, internet gaming, e-mail spamming, cyber phishing, cyber harassment, unlawful access to computer systems, stealing of information stored in electronic form, e-mail bombing, physically destroying computer systems, and so on are all examples of cybercrimes.[75]

The numbers that have been gathered and reported on show how widespread Internet crimes are around the world. Phishing emails alone bring in one billion dollars for the criminals who send them. In a survey conducted by the FBI in early 2004, 90 percent of the 500 businesses surveyed said they had experienced a security breach, with 80 percent of those saying they had suffered a financial loss.[76] According to a nationwide estimate from 2003, four billion dollars were spent per year due to credit card theft. Just 2% of credit card transactions are done over the Internet, but they account for half of the four billion transactions listed earlier.Many of these findings serve as examples of how the Internet is being abused and that Internet violence must be curtailed.

4.4ARTIFICIAL INTELLIGENCE

In July 1956, at Dartmouth College's Summer Science Project, AI (then known as machine intelligence) became a research discipline. The concept was coined by John McCarthy, who describes it as "the science and engineering of creating intelligent machines." "Artificial Intelligence is the exploration of how to make machines do stuff that humans do better at the moment," according to a widely agreed description.[77] Reasoning, information, organizing, listening, natural language processing (communication), vision, and the capacity to move and control objects are all key problems (or goals) in AI science. Three capabilities are required of an AI system.

i. Save information;

ii. Use the information to fix problems

iii. Gain new skills by practice.

Representation, Reasoning, and Learning are the three main components of AI.[78]

The challenge of simulating intelligence has been broken down into smaller sub-problems, each of which has unique features or attributes that an intelligent machine should have. The following characteristics have received the most attention:

a) Deduction, reasoning, problem solving

b) Knowledge representation

c) Planning

d) Machine learning

e) Natural Language Processing

[75] Halder, D. Jaishankar, K, "Cyber crime and the Victimization of Women: Laws, Rights, and Regulations". Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

[76] VineetKandpal and R. K. Singh, "Latest Face of Cybercrime and Its Prevention In India", International Journal of Basic and Applied Sciences, Vol. 2, Pp. 150- 156, 2013

[77] V. Rajaraman, "John McCarthy – Father of Artificial Intelligence", in General Article Resonance, March 2014

[78] T N Shankar, Neural Networks, LAXMI Publications Pvt. Ltd, 2008

f) Motion and Manipulation

g) Perception

h) Social Intelligence

i) Creativity

j) General Intelligence

Individual human actions, information interpretation, and inference techniques are the core focuses of traditional AI approaches. Distributed Artificial Intelligence (DAI), on the other hand, is mostly concerned with social activity. DAI systems are cooperative systems in which a group of agents works together to solve a problem. These agents are often diverse. "An agent may be a real or virtual being that can function, interpret its environment (in a partial way), interact with others, is autonomous, and has skills to accomplish its aims and tendencies," writes Jacques Ferber (1999).[79]Agents are discrete entities with specified borders and interfaces that are used to solve problems. A multi-agent scheme, on the other hand, is a loosely connected network of agents that function as a single unit, similar to a society, to solve problems that an independent agent cannot. The following are the major implementations of multi-agent systems:

- Problem Solving
- Multi-Agent Simulation
- Synthetic World Construction
- Collective Robotics
- Kenetic Program Design

Computational Intelligence (CI) is a branch of AI that focuses on heuristic algorithms including fuzzy systems, neural networks, and evolutionary computation. The terms "Soft Computing" and "Computational Intelligence" are synonymous. Computational Intelligence has recently expanded to include new fields such as artificial immune systems, swarm intelligence, chaotic systems, and so on. Neural networks, fuzzy logic, evolutionary computation, swarm intelligence, deep learning, and artificial immune systems are examples of nature-inspired approaches that offer versatile decision-making mechanisms for problems like cyber security.[80]

Another kind of AI technique is genetic algorithms. Also for complex computing problems, they have reliable, scalable, and optimal solutions. They can be used in intrusion detection systems to generate guidelines for classification of security attacks and to create new rules for various security attacks (IDS).

4.5INTRUSION DETECTION AND PREVENTION SYSTEM

Where traffic does not pass through the firewall at all, an Intrusion Detection System (IDS) can provide protection against external users and internal attackers. The

[79] J. S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, Upper Saddle River, Prentice Hall, New Jersey, USA, 2003

[80] Jacques Ferber, Multi-Agent System: An Introduction to Distributed Artificial Intelligence, Harlow: Addison Wesley Longman, 1999

firewall protects an organisation against disruptive Internet threats, and the IDS detects whether anyone attempts to hack through the firewall or manages to break through the firewall protections to gain access to some device on the trustworthy hand. If there is a security violation, it notifies the system administrator. An IDS is similar to a smoke detector in that it can sound a warning if such conditions are met.[81]

An Intrusion Detection System (IDS) is a computer or piece of software that tracks network or system activity for malicious activity or policy breaches and sends notifications to a management station. Network-based Intrusion Detection Systems (NIDS) and host-based Intrusion Detection Systems (HIDS) are two types of IDS (HIDS).

IDS executes a number of tasks, including:

- Auditing system configuration for vulnerabilities and misconfigurations
- Assessing the integrity of critical system and data files
- Recognizing known attack patterns in system activity
- Identifying abnormal activity by statistical analysis
- Managing audit trials and highlighting user policy violations or normal activity

An intrusion detection and prevention system (IDPS) is a software or hardware unit that is installed within a network that can detect and avoid intrusions.[82]

When compared to conventional approaches, Artificial Neural Networks (ANNs) can improve the efficiency of Intrusion Detection Systems (IDS). In the search for artificial intelligence, artificial neural networks are a turning stone. ANNs are information retrieval systems that are modeled after the biological nervous system. We can build AI using the tools provided by ANN.

4.6APPLICATIONS OF AI TECHNIQUES IN DEFENDING CYBER CRIMES

AI methods have a wide range of uses in cybercrime identification and mitigation, according to scholarly resources. For example, neural networks may be used to create a highly effective intrusion detection and prevention method. There is also a proposal for using artificial neural networks in the analysis of DoS attacks, computer worms, spam, and zombies, as well as malware recognition and forensic examination.[83] To increase their performance, next generation antivirus programs employ AI techniques such as data mining, neural networks, and heuristics approaches. Intelligent agents and mobile agents are also used in distributed wireless intrusion detection systems (IDS). IDS focused on mobile agents offer

[81] N. A. Alrajeh and J. Lloret," Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, Vol.2013, Article ID 351047.

[82] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, A. Patel, "An appraisal and design of a multiagent system based cooperative wireless intrusion detection computational intelligence technique," Engineering Applications of Artificial Intelligence, Vo. 26, pp. 2105–2127

[83] X. B. Wang, G. Y. Yang, Y. C. Li and D. Liu, "Review on the application of Artificial Intelligence in Antivirus Detection System", In Proceedings of the IEEE Congress on Cybernetics and Intelligent Systems, pp. 506-509,2008

network protection by incorporating accessibility capabilities into the detection of malicious cyber behavior.

4.6.1APPLICATION OF ARTIFICIAL NEURAL NETWORKS AGAINST CYBER CRIMES

An Artificial Neural Network (ANN) is a massively parallel distributed processor made up of basic processing units that has a built-in capability for storing and retrieving experimental information. Chen (2008) presented NeuroNet, a neural network device capable of tracking flow, detecting traffic disturbances, and initiating countermeasures. NeuroNet is successful against one form of secret attack known as low-rate TCP targeted distributed DoS attacks, also known as shrew attacks, according to the findings of the NS-2 experiment.[84]

Iftikhar et al. (2009) developed an ANN-based method for detecting probing attacks. It used a supervised neural network phenomenon to test the viability of a method for probing attacks in computer network networks that are the foundation of other attacks. When the evolved framework is subjected to various probing attacks and its efficiency is compared to that of other neural network approaches, the results show that the approach based on Multiple Layered Perceptron (MLP) architecture is more detailed and reliable, and that it produces the best results when compared to other methods.

Linda et al. (2009) presented a novel IDS-NNM – Intrusion Detection System using Neural Network based Modeling – that employs a unique combination of two neural network learning algorithms for behaviour modeling, namely Error-Back Propagation and Levenberg-Marquardt. The IDS-NNM algorithm is capable of catching all intrusion attempts posed in network communication without producing any false alarms, according to experimental findings.[85]

With the aim of improved performance, Barika (2009) proposes an Artificial Neural Network architecture for decision making within intrusion detection systems.

Brij is a word that comes to mind when (2011) An ANN is used to approximate the amount of zombies involved in a flooding DDoS attack, which is useful in reducing the attack's effect.[86]

Wu (2009) proposed a spam filtering approach that combines rule-based computation and back-propagation neural networks. This technique has proved to be much more robust than other spam detection methods that consider keywords, since spamming patterns can alter frequently.[87]

Kufandirimbwa and Gotora (2012) proposed a spam filtering strategy based on Artificial Neural Networks and the perception learning process, which has higher detection rates than other spam detection methods based on text and other message characteristics due to the inclusion of a continuous learning function.

[84] M Rajesh Kanna, D. Hemapriya and C. Divya," Intelligent Agents For Intrusion Detection System (IAIDS)", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 3, January 2013. [21]N. Jaisankar, R. Saravanan, K.DuraiSwamy, "Intelligent Intrusion Detection System Framework Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol 1, July 2009

[85] Yu Chen, "NeuroNet: Towards an Intelligent Internet Infrastructure", In Proceedings of the 5th IEEE Congress on Consumer Communications and Networking Conference (CCNC), pp. 543 547,2008

[86] BrijBhooshan Gupta, Ramesh Chand Joshi, and Manoj Misra, "ANN Based Scheme to Predict Number of Zombies in a DDoS Attack", International Journal of Network Security, Vol.14, PP. 61–70, Mar 2012

[87] Ondrej Linda, Todd Vollmer and Milos Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures", In Proceedings of the International Joint Congress on Neural Networks, 2009

Zhai (2014) suggested a multi-agent distributed IDS (DIDS) paradigm for intrusion detection based on BP neural networks, which has the benefits of reducing the amount of mobile data processing, load balancing, neatly detecting analysis, better error-tolerating, and effectively detecting distributed intrusion.

4.6.2APPLICATION OF INTELLIGENT AGENTS AGAINST CYBER CRIMES

Intelligent agents are self-contained computer-generated forces that can interact with one another and exchange data, as well as collaborate to prepare and execute effective responses in the event of unpredictable events. Intelligent agents are well-suited to countering cyber attacks because of their versatility, adaptability in their deployment environments, and collaborative existence.

Using multiagent preparation and some innovative inference approaches, Rowe (2003) created a technique to systematically counter plan the ways to deter specific cyber attack plans.

Helano (2006) presented a Prolog-oriented architecture that is a synthesis based on a multi-agent systems (MAS) approach, with a realistic argument for fighting cyber intrusions and the potential to validate cybercrime assets.[88]

Mueen Uddin et al. (2010) introduced a modern paradigm called Dynamic Multi-Layer Signature based IDS with Mobile Agents, which can identify imminent threats with a high success rate by dynamically and automatically building and utilizing tiny and effective multiple databases, with a method to upgrade these small signature databases at frequent intervals using Mobile Agents.

To address the shortcomings of current Mobile Agent-based Intrusion Detection Systems, Onashoga et al (2013) suggested a Multi agent-based architecture for Intrusion Detection System (IDS) with three main phases: data gathering, detection, and response.

M. Rajesh Kanna et al. (2013) created a wireless distributed Wireless Intrusion Detection System (WIDS) focused on Intelligent agents with four main components: Intrusion detection module, Warning, Mobile agent platform, and Test suit.[89]

4.7AI FLEXIBLE FEATURES FOR IDPSs

AI strategies have a number of characteristics that make them ideal for building an intrusion detection and prevention scheme.

Technologies and their features:

1. Artificial Neural Networks
   i. Learning by example.
   ii. Resilience to noise and incomplete data.
   iii. Intuitiveness since it mimic biological neuron.
2. Intelligent Agents

[88] IftikharAhmad, Azeen Abdullah, and Abdullah Alghamdi, “Towards the selection of best neural network system for intrusion detection”.

[89] BrijBhooshan Gupta, Ramesh Chand Joshi, and Manoj Misra, “ANN Based Scheme to Predict Number of Zombies in a DDoS Attack”, International Journal of Network Security, Vol.14, PP. 61–70, Mar 2012

    i. Mobility.
    ii. Adaptability.
    iii. Collaboration
3. Artificial Immune Systems
    i. Self-adaptability.
    ii. Self-organizing.
    iii. Dynamic nature
4. Genetic Algorithms and fuzzy
    i. Optimization.
    ii. Robustness.
    iii. Flexible

4.8 LIMITATIONS OF EXISTING ANOMALY DETECTION AND PREVENTION SYSTEM

IDPS have been increasingly useful in improving the reliability of networks and end hosts in recent years; however, they have a number of significant disadvantages.[90] They are as follows:

- Encryption: After data packets have been secured, current security systems can be rendered useless in detecting intrusions.
- Signature evasion: polymorphic worms that can change their propagation properties and hence their signatures automatically. These worms are also a serious threat to the existing detection scheme.
- False Positives: A false positive occurs when an intrusion detection system (IDS) incorrectly raises a security hazard warning for innocuous traffic.
- Regulatory requirements: intrusion detection devices must adhere to legal requirements.
- IDPS attack: if attackers can figure out how the device operates, they can be able to kill it.

4.9 LET'S SUM UP

Since we now live in an interconnected environment, the majority of our daily conversations and business operations are now conducted over the Internet.

[90] ZhaiShuang-can, Hu Chen-jun and Zhang Wei-ming, "Multi-Agent Distributed Intrusion Detection System Model Based on BP Neural Network", International Journal of Security and Its Applications Vol.8, pp.183- 192, 2014.

However, it has resulted in difficult-to-manage problems, such as the rise of cybercrime. Academic tools reveal that AI methods are now being used to tackle cybercrime in a variety of ways. We've briefly discussed the capabilities of AI strategies in the area of cybercrime so far, as well as their existing shortcomings.

4.10FURTHER READING

- Selma Dilek, HüseyinÇakır and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015.
- JheelSomaiya, DhavalSanghavi, ChetashriBhadane, "A Survey: Web based Cyber Crimes and Prevention Techniques", International Journal of Computer Applications (0975 – 8887), Volume 105, November 2014.
- Halder, D. Jaishankar, K, "Cyber crime and the Victimization of Women: Laws, Rights, and Regulations". Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.
- VineetKandpal and R. K. Singh, "Latest Face of Cybercrime and Its Prevention In India", International Journal of Basic and Applied Sciences, Vol. 2, Pp. 150- 156, 2013.
- J. S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, Upper Saddle River, Prentice Hall, New Jersey, USA, 2003.
- Manveer Kaur, ShevetaVashisht, Kumar Saurabhi, "Adaptive Algorithm for Cyber Crime Detection", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (3), 4381 – 4384, 2012.
- M Rajesh Kanna, D. Hemapriya and C. Divya," Intelligent Agents For Intrusion Detection System (IAIDS)", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 3, January 2013. [21]N. Jaisankar, R. Saravanan, K.DuraiSwamy, "Intelligent Intrusion Detection System Framework Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol 1, July 2009

4.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is an Intrusion Detection System?**

An Intrusion Detection System (IDS) is a computer or piece of software that tracks network or system activity for malicious activity or policy breaches and sends notifications to a management station.

2. **What is an Intrusion Detection and Prevention System?**

   An intrusion detection and prevention system (IDPS) is a software or hardware unit that is installed within a network that can detect and avoid intrusions.

3. **What is ANNs?**

   ANNs are information retrieval systems that are modeled after the biological nervous system.

4.12 ACTIVITY

1. Discuss about IDPS and how are they able to contribute in the prevention of cybercrimes. (400-500 words)
2. Critically analyse the AI's role in the protection of cybercrimes. (1200-1500 words)

Block-3

DATA PROTECTION AND PRIVACY

1

Unit 1: AI AND PRIVACY LAW

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- the unrealized value of Learned Intelligence
- Artificial Intelligence and Computer Vision
- how Learned Intelligence affects the Insurance Industry

1.2 INTRODUCTION

Manufacturers and service providers are now faced with previously unconsidered ways to extract benefit through the reuse and repurpose of data originally gathered and harvested for other purposes, thanks to the exponential proliferation of technology through any area of business.[91] Artificial intelligence (AI) systems add meaning to the processor that had not previously been understood or accepted in transactions. This is especially relevant when it comes to how AI firms who partner with insurers to improve claims management are left with a valuable resource after the data is collected.

1.3THE UNREALIZED VALUE OF LEARNED INTELLIGENCE

Data protection and privacy have been hot topics in the business world, civil rights groups, and even sovereign nations over the last decade. Massive data leaks have disclosed confidential details, government hackers have revealed classified information, and internet hacks have revealed nude celebrity images and the use of discreet dating apps for extramarital affairs. The founder of Facebook was summoned to appear before Congress on the subject of privacy. The European Union and the state of California, among others, have adopted comprehensive laws to regulate people's privacy and data access.[92] Despite this, the corporate world continues to search for productivity nirvana – the use of data for specific activities. The insurance sector, which is one of the most heavily regulated sectors in terms of anonymity, has recognised the importance of data and is working to build on it. With the increased use of AI in the analysis of such data, the industry must consider a number of considerations when engaging in transactions involving such data.

People have practiced Sir Francis Bacon's theory of "scientiapotentiaest," a Latin aphorism that means "intelligence is force," for more than 400 years. Companies depend on analytics to advise their operations, managers, and strategies now more than ever to increase their market strength. The development in artificial intelligence (AI) over the last 60 years has had a huge effect on our daily lives. When one opens a Facebook newsfeed, conducts a Google search, or receives a suggestion from a well-known website, AI is at work.AI is used by consumers who use robotic vacuum cleaners or navigation software to help them find the right way. Amazon, a household name in most Americans' lives, has expanded its company largely thanks

[91] Shrikant, Ardhapurkar& Srivastava, &Tanu, & Swati, Sharma &chaurasiya, Mr &Vaish, Abhishek. (2010). Privacy and Data Protection in Cyberspace in Indian Environment. International Journal of Engineering Science and Technology. 2.

[92] Privacy-Enhancing Technologies—approaches and development http://www.sciencedirect.com/

to artificial intelligence. But, what's the big deal? AI seems to be changing our lives, with improved health services, financial management, and a better social climate on the horizon.

When AI is mixed with questions over data protection and possession, a problem emerges. We're discussing the importance of info, which has been dubbed the "fresh" oil. Clive Humby, the British mathematician behind Tesco's Clubcard rewards scheme and My Kroger Plus, is credited with coining the phrase "information as an asset, equal in worth and usefulness to gasoline."[93] Although data is intrinsically useful, it must be processed, just as oil must be refined before it can achieve its full value, according to Humby. Data is used to power transformative developments in the same way as oil has fueled industrial development. Data has many benefits, including the ability to be conveniently transported and reused at a low cost. Furthermore, unlike oil, data can become more valuable the more it is used. As a result, data is equivalent to and more useful than oil in several respects.

Having said that, the concept of data manipulation has been somewhat concrete and observable until recently. Data is created by processes, which are then siloed by departments and stored in databases or filing cabinets, or by a series of processes. This data is typically easy to locate, inspect, and monitor, especially when it is used and handled by contracts and outsourcing agreements. The data can be picked up, reused, and transferred to a new process, or it can be outsourced and reused. Customers purchasing and renewing insurance from a website, for example, may be transferred into an application with some preparation for a better or different user experience. Although the content of data has not improved, the concept of data interconnection is encouraging new applications of analytics, ranging from stock trading to professional sports. Data has a primary function, and its interrelationship with other data has a certain role.

When a motorist is involved in a car crash, the insured records information such as the model of vehicle, the injury, the site of the accident, the driver, the passenger, and the conditions, to name a few. Much of this information is used to process the collateral loss petition, as well as any possible physical injury and medical insurance claims. However, as this data is exposed to algorithms and artificial intelligence, it may be used for other purposes.[94]

If a motorist is involved in a car crash, data can theoretically be aggregated to draw some conclusions when the data is linked to other data. For instance, the type of car and the injury it sustains can be used to draw conclusions about the safety of vehicles involved in collisions, the cost of property damage, and also the risk of being involved in a "accident." The accident's location will aid in the identification of hazardous places and road conditions. The identities of the drivers and passengers, as well as the injuries they suffered, will be used to assess if cars are adequately equipped with safety features. The list continues on and on. The argument is that the information gathered isn't only helpful with the accident in question; it can even be used for a variety of different things when combined with other information. The data gathered from these analytics will be beneficial to the collector and researcher. It is

[93] Philip E. Agre, Marc Rotenberg Technology and privacy: the new landscape http://books.google.co.in/books?id=H2KB2DK4w78C&printsec=frontcover&dq=technology+and+privacy&source=bl&ots=1UZmu8TrQp&sig=YJJNgSU61_nTcL_CnCl7Je2LcrQ&hl=en&ei=7L2YS_T2KYSysgOygbnCAQ&sa=X&oi=book_result&ct=result&resnu m=2&ved=0CAkQ6AEwAQ#v=onepage&q=&f=false

[94] White Paper on Privacy Protection in India :Vakul Sharma http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy. %202007.pdf

valuable and referred to as “oil.” However, who owns the data and how useful it is is up for debate.

1.4COMPUTER VISION AND AI: WHO OWNS THE NEURAL NETWORK

AI technology has the potential to drastically alter industries and operations, just as the steam engine and assembly line did with production. Company sees potential benefit in the opportunity to ramp up without incurring large human costs. This untapped productivity and “knowledge capacity” is being commoditized and accepted as a valuable resource.AI technology has the potential to drastically alter industries and operations, just as the steam engine and assembly line did with production. Company sees potential benefit in the opportunity to ramp up without incurring large human costs. This untapped productivity and “knowledge capacity” is being commoditized and accepted as a valuable resource.[95]

Businesses must be aware that if they outsource incorrectly, they risk losing control of the data and systems they outsource. Since AI’s commoditization of data is only in its early stages, these companies would have a competitive advantage. Waiting one, two, or three years to correct data control and commoditization could result in a major setback, given the widespread acceptance of data and AI. It may also be too late; businesses may never recover control of the same companies they once considered friends and allies.

It’s a basic concept: if you have one thing and someone gives you another, you now have two. If you send somebody water and salt, they will render salt water. When the salt is taken out, the person still knows how to make salt water even if the ingredients are no longer available. When using an AI method, if a neural network is given data and the computer absorbs information from its analysis, the machine still has the value of the acquired wisdom even if the data is deleted.

The ability to transfer data is evolving, and new outsourcing agreements can jeopardize a company’s ability to efficiently move and tailor its processes to how it needs things done or how its customers want things done.

1.5THE VALUE OF LEARNED INTELLIGENCE IN THE INSURANCE INDUSTRY

Let’s have a look at how a traditional insurance provider has dealt with upgrading and improving the claims process in recent years, especially the usage, value, and handling of data within that process. Although each business has its own procedure, this review is founded on a common methodology and understanding.[96]

Until about 60 years ago, insurance firms were responsible for contract issuing and placement, as well as managing all lawsuits. The administration of the claims process was then taken over by firms including Crawford and Co. and Gallagher Bassett. Third-party managers (TPAs) added structure and size to the claims

[95] SAFE HARBOR PRIVACY PRINCIPLES
http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/national%20laws/1USA_SAFE%20HARBOR%20PRIVACY%20PRINCIPLES.pdf

[96] Data Protection Technical Guidance Note: (PET) Privacy enhancing technologies (ICO)
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.pdf

resolution process. This was also combined with the use of outsourcing to countries like India, the Philippines, and other low-cost locations. After the 1980s, the principle of outsourcing has evolved significantly.

According to Fortunly, an organization "dedicated to demystifying financial processes, interpreting terms, and breaking down complicated transactions into basic measures," Nearly 54% of all businesses use third-party support teams to communicate with clients, and more than 93% of businesses have implemented or are exploring cloud platforms to increase outsourcing. Although data protection is a top priority for 68 percent of outsourcing firms exploring cloud adoption, more than "44 percent of chief intelligence officers report they are more likely to use outsourcing vendors than they were only five years ago."

In terms of claims management, outsourcing to a TPA or offshore still provided for a high level of process control. From the perspective of an insurance firm, it also owned and controlled the records, could customize the operation, and take advantage of size and cost savings. The insurer could travel to India or pay a visit to the TPA and direct its claims to the appropriate team. The data was also stored in files (databases) and maintained by departments inside the TPA or outsourcing company.[97]

Personnel and the main process is under the jurisdiction of the TPA, but the data could be picked up and transferred to another TPA, or even taken back in-house or outsourced again. Claims are routinely outsourced to lower-cost regions or businesses. The insurance carrier retains ownership of the data and the process at this stage, owing to the fact that it is manual or, at best, computer-based through some form of process automation. The insurance company's right to control or drive the process remains unaffected.

The TPA's key value proposition to insurers is expense, size, and management of the staff and team responsible for handling claims and adding value through their claim settlement expertise. The value of the TPA and the value of the insurance company are distinct.

With the integration of AI and machine learning into the claims process, a new breed of digital TPA, an AI enterprise, is emerging. On the surface, the value proposition seems to be the same as before, but with greater scaling potential and cost savings. The new business can provide opportunities to fundamentally alter how an insurer views risk. There is, though, a catch that you might not have seen before now. Although the TPA/AI firm might be providing a service, it is also acquiring an advantage that was previously unrealized and perhaps unaccounted for before the TPA/AI firm began its partnership with the insurance firm. When data is analyzed by an AI-powered TPA, insurance providers should be aware of the changing importance of data processing. The TPA may receive the value of the information gained from the data, and the insurer may lose a valued asset.

The TPA's AI technologies must be conditioned on the insurer's claim data in order to become professional at a particular mission. This may be the method of feeding data to the AI in the form of images, places, and words in order to train the neural network and create awareness. The insurance company's "data" feeds into the neural network. This training enables AI technology to function and succeed. The more data there is, the better the AI will be at performing the task. This technology is highly versatile and extremely useful. The value of learned knowledge could

[97] Under Pressure, India Mulls Steps to Protect Privacy (Vir Singh) http://spectrum.ieee.org/telecom/security/under-pressure-indiamulls-steps-to-protect-privacy

eventually dwarf the value of individual details, similar to the adage, “Give a man a fish, and you feed him for a day; teach a man to fish, and you feed him for a lifetime.”

The transition from using a TPA to populating a neural network with an AI-powered TPA is subtle but important. Building a project with a TPA to train an AI on the promise of faster claims settlement is good and efficient, as long as the insurance provider knows the benefit transfer as well. If this is what is explicitly understood in the contract, the value transfer should be quick and clear: the insurer gets an automatic process, and the AI business gets to develop AI applications that can scale on the insurer’s data. But, does the insurer realize that, while reaping the benefits of AI, it is still constructing a potentially strong brain for the outsourced service, making it possible for those to contend with it?

If the TPA uses a typical neural network, it is creating this “brain” using data from the insurance industry, and this acquired wisdom will never be returned to the insurance company without the TPA discarding its hard work and neural network. When a TPA handles claims for multiple insurers or self-insured entities, the experience and processes of one insurer/self-insured entity are leveraged for the good of the others. Although the images and other data that the TPA input and processed can be returned or discarded (as expected by certain service contracts), the data that filled and educated the neural network leaves acquired intelligence with the TPA that is difficult to erase.[98] If the learned intelligence is not returned or lost, the stored data may be resold to other insurers and self-insureds via the TPA’s services. As TPAs may boast that they provide more intelligence than every other insurer, the power shifts from a TPA simply providing an outsourced opportunity to a TPA providing an insurer with more knowledge and insights based on “industry” data derived from the original insurer’s processed data.

The presence of a common neural network also lowers the entry barrier for new insurers, who can simply hire an AI-powered TPA to handle claims without having to provide any initial details.[99] A new entrant no longer requires the expertise required to develop a massive claims enterprise in order to advise its underwriting and claims settlement. This ease of entry into the insurance industry can encourage well-capitalized financial and technology firms to enter the market as new insurance players, challenging long-established firms that have invested decades in their own processes.

1.6NEGOTIATE WITH UNDERSTANDING

Many insurers may decide not to invest capital or professional personnel in developing an automated AI claims process. As a result, they’ll have to outsource this task. Without the vast databases and learned expertise of insurers, an AI business would fail to have the claims automation that the insurer requires; as a result, the AI company and the insurer would need to collaborate.[100]The use of an AI-powered TPA arrangement by an insurer may be a perfectly suitable strategy. However, the parties to this transaction should be aware of whether the TPA is utilizing a common neural network, whether the learned intelligence can or should be

[98] Bob Whitehead, Invasion of privacy laws and video surveillance -- what’s legal, what’s not? http://www.video-surveillanceguide.com/3048-invasion-of-privacy-laws.htm

[99] Roger Clarke Visual Surveillance and Privacy http://www.rogerclarke.com/DV/VisSurv0508.html

[100] Tracy Mitrano, Civil Privacy and Legislative Security Policy http://net.educause.edu/ir/library/pdf/ERM0362.pdf

discarded, and whether it is entitled to the residual value of the learned intelligence acquired by the TPA as a result of the data processing. The transaction's parties must know the best questions to pose, have a shared sense of the importance of the learned information, and each party's understood objectives must be clear and contractual. The advantages of AI in the claims handling process and in underwriting may become ever more important in the years ahead, regardless of whether an insurer uses a common neural network or a segregated neural network. Rather than waiting for a contract to expire, the insurer and its AI-powered TPA should be constructive, recognizing and addressing these problems right away.

1.7 LET'S SUM UP

We have learnt about how artificial intelligence is used and how it can compromise your privacy if it's not handled properly. The TPAs need to be set up in such a way that the insurers will benefit from them.

1.8FURTHER READING

- Lin, J. C. W., &Yeh, K. H. (2021). Security and Privacy Techniques in IoT Environment.
- Bartneck, C., Lütge, C., Wagner, A., & Welsh, S. (2021). Privacy Issues of AI. In An Introduction to Ethics in Robotics and AI (pp. 61-70). Springer, Cham.
- Michael J Quinn. Ethics for the information age (7th edition). Addison- Wesley Publishing Company, 2017. ISBN 978-0134296548 (Chap. 5).
- SareBaase and Timothy M. Henry. A Gift of Fire Social, Legal, and Ethical Issues for Computing Technology (5th Edition). Prentice Hall PTR, 2017. ISBN 9780134615271 (Chap. 2).

1.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is a Third-Party Administrator (TPA)?**

   A third-party administrator is an organization that contracts with another company to offer operational services such as claims administration and employee health administration. Claims management is frequently outsourced by insurance providers and self-insured businesses.

1.10 ACTIVITY

Elucidate the relationship between AI and data privacy along with examples. (1000-1500 words)

Unit 2: DATA PROTECTION AND PRIVACY PROTECTION ON PUBLIC CLOUD

2

Unit Structure

2.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- security issues relating to cloud architecture
- data integrity protection methods
- data privacy protection methods

2.2 INTRODUCTION

Because of its on-demand service and scalability capabilities, cloud computing has become a common technique. The cloud is most often used for data collection and big data or computation-intensive systems today. As a result, data protection and privacy has become a top priority, especially for business-related data. Data protection, transparency, and integrity are the three core aspects of data protection. The aim of data protection is to keep data collected in the cloud from being identified.[101] Data protection and privacy challenges remain in the cloud in the data life cycle, from generation to upload, usage, exchange, preservation, and archival.Data encryption and access management are often used with traditional data protection systems. And if the adversary obtains the data, data protection using AES or other encryption techniques will avoid valuable information from being leaked. However, due to high encryption and decryption overhead in storage and computing, it has reliability issues when working with oceans of data in a cloud world. The aim of access control is to deter unauthorized users from gaining access to records.[102]

However, in cloud computing, users may not have physical control of the machines on which they store data, and since the same physical machine can be used by multiple tenants thanks to virtualization, an adversary may monitor physical machine behavior to obtain valuable data from other tenants, and cloud providers are unreliable, they can accidentally or intentionally compromise data. Many studies have been conducted on the unique aspects of data protection in the cloud computing environment.

2.3CLOUD ARCHITECTURE AND SECURITY ISSUES

Both outsider and insider attacks pose a challenge in a public cloud world. Malicious code attacks, DDoS attacks, network eavesdropping, and so on are all examples of outsider attacks. The cloud infrastructure architecture has three levels. Each physical computer has several virtual machines (VMs) built in the infrastructure layer. Customers are provided with a portal by the platform layer. Customers can have their own software, programs, and configurations installed. The cloud vendors provide the software stacks across the software layer.A consumer on the client side may be a legitimate user or an actor impersonating legitimate users. Man-in-the-

[101] G. Ateniese, M. Steiner, and G. Tsudik ," Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," IEEE Trans. on Cloud Computing,2015.

[102] Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou , "Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, vol . 25, issue. 1, 2014.

middle threats may also be carried out by network eavesdroppers.[103] To secure the whole cloud network, firewalls or intrusion detection systems (IDS) may be mounted. In the following chapters, we'll go through potential threats at various points and how to defend yourself.

a) Authentication:

End users and the cloud environment are all vulnerable to attacks during authentication. For authentication, most public cloud services today, such as AWS, use public/private keys. Users must first build and download a key pair created after logging in with their username and password. The key pair is used for further connection and authentication to EC2 instances.[104] However, in the middle of the network, eavesdroppers can intercept the main pair and do crypto analysis or a man in the middle attack. In this case, periodically updating the key pair and using multifactor authentication can be beneficial.

b) Virtual Machine Attacks:

Many tenants will use the same physical computer in the public cloud due to virtualization. If adversaries posing as legitimate users gain access to the virtual computers, they will be able to carry out attacks for the following reasons:

- Calls to a virtualized network interface are routed to a real network device. If malicious code is inserted, it can spread to other virtual machines on the same physical computer, and possibly to other physical machines.
- An adversary may execute attacks using relaxed access control and inter-VM contact on the same physical computer.[105]

c) DDoS attacks:

Since cloud services have a large number of servers, it will be difficult for attackers to launch DDoS attacks. However, once the opponent knows the location of the data, they will make the individual servers that host the user's data unavailable to access. Live virtual machine migration may be used to solve this problem. AWS, for example, offers a Virtual Private Cloud (VPC) solution for tighter access management.

d) Insider abuse:

Unlike single computers and pools, cloud computing machines are owned by cloud companies. Cloud vendors must have a good understanding of the data's contents, location, and computation/analytics approaches. Data stored in the cloud may be leaked if cloud vendors collude with adversaries. As a result, strategies for securing data in untrustworthy cloud services must be created. In the following pages, we'll go through some of the current processes, such as multiple storage.[106]

[103] Dev, H., Sen, T., Basak, M. , Ali, M.E. "An Approach to Protect the Privacy of Cloud Data from Data Mining Based Attacks", High Performance Computing, Networking, Storage and Analysis , pp. 1106 – 1115, 2012.

[104] K. Hwang and D. Li, " Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, Vol.14, Sept. 2010.

[105] Yang Pan; GuiXiaolin; An Jian; Yao Jing; Lin Jiancai; Tian Feng , "A retrievable data perturbation method used in privacy-preserving in cloud computing", China Communications, vol. 11, issue 8, pp. 73-84, 2014

[106] Ming Li; Shucheng Yu; Kui Ren; Wenjing Lou; Hou, Y.T, "Toward privacy-assured and searchable cloud data storage services", IEEE Network, vol. 27, issue. 4, pp.56-62, 2013.

2.4CLOUD DATA SECURITY CHALLENGES

As previously said, there will be more data protection issues in a cloud setting than in a conventional single machine that is in the hands of the customers. Various issues and potential threats during cloud data use and storage processes are summarized in this section.

a) Data Use

As data is moved to the cloud, cloud administrators can have full access to everything customers have converted to cloud machine instances. The data collected in the cloud may be misused by both opponents and cloud vendors. As a result, data transformation will be required to avoid the loss of useful knowledge. Simple encryption is possible if the cloud is only used for data storage and no other operations are needed.[107]

However, in most cases, additional processing is needed. Users may need to do some processing on the data they've saved. Computations such as matrix multiplication, for example, may be required. For data classification, data mining approaches such as machine learning algorithms must be used.

The cloud is where data computation and analytics take place. However, some cloud data applications will necessitate coordination between local users and the remote cloud. Users can, for example, require the retrieval of specific data in order to modify it using data querying.

The below is a detailed description of the above cloud data use concern:

1) Encrypted data processing. The algorithms for data and computation-intensive software are often stored in the cloud. Cloud providers may deduce what types of data are processed based on the algorithms. Furthermore, in order to secure privacy, the data to be stored must be encrypted. The topic of how to process encrypted data without decryption remains unanswered.
2) An attack on query analytics. Significant amounts of data are stored in a cloud environment.[108] For auditing, sorting, or other processes, remote users must query data hosted in the cloud. For the following purposes, queries may be used to carry out attacks:
    a) These requests and queried answers will be obtained via an Internet link with eavesdroppers sitting in the centre.
    b) The cloud vendor is untrustworthy. Cloud providers have little visibility into the data handling procedures. Even if the original data is transformed

[107] Boyang Wang; Baochun Li; Hui Li, " Oruta: privacy-preserving public auditing for shared data in the cloud", IEEE Transactions on Cloud Computing, vol.2, issue. 1, pp. 43-56, 2014

[108] AlexandruButoi, NicolaeTomai, "Secret sharing scheme for data confidentiality preserving in a public-private hybrid cloud storage approach", 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing

and stored within, and the same query is translated to different values per time and sent to the cloud world, cloud providers will still be able to extract any information.

c) Prior knowledge of the data gathered from open databases may be paired with the empirical findings to derive useful details.

b) Data Storage

Users' data is maintained in remote virtual machine instances owned by service vendors in a cloud environment. External attacks on virtual machines may include malicious code attacks, breaching the associated Virtual Machine Monitor, and so on. Aside from the threat from the outside, consumers have no physical control over their files. Cloud providers' insiders could see just what was stored in their virtual machine instances. It would be a disaster if cloud providers' insiders collaborated with rivals to alter or leak customers' data on purpose.

Confidentiality, honesty, and availability are all aspects of data storage protection. How to avoid information theft and effectively verify data privacy over vast amounts of data stored in the cloud remains a concern in terms of data confidentiality. The aim here is to reduce the chances of recovering the original data from the hacked cloud storage system. In order to maintain data confidentiality, opponents and cloud vendors will purposefully alter the data. It is important to perform effective integrity checks on massive amounts of data. Customers' data will be inaccessible due to both system maintenance and threats in terms of data availability.

2.5DATA INTEGRITY PROTECTION METHODS

Data Modification Attack, Tagforgery and Data Leakage Attack, Replay and Timeliness Attack, Roll-Back Attack and Collusion Attack, and Byzantine Attack are all examples of data confidentiality attacks in the cloud. To maintain secrecy and integrity, a Trusted Cloud Computing Platform (TCCP) built on trusted computing is suggested. Each node has the trusted framework module installed. However, since users do not have power over the physical equipment, remote attestation is needed to ensure that the calculation comes from the virtual machine on which users are operating applications.[109]

A trusted platform module (TPM) is inserted in each virtual machine, and a trusted virtual machine monitor (TVVM) is enabled during booting. Furthermore, the attestation is performed by an external trustworthy coordinator (TC). Digital nodes must first register with TC. TPM-based Intel Trusted Execution Technology (TXT) is already available. It's compliant with OpenStack, an open-source cloud computing software framework. It contains an Open Attestation registry that communicates with the trusted computing pool of hardware and software. With trusted cloud storage,

[109] Y. Kajiura, A. Kanai, S. Tanimoto, and H. Sato, "A file distribution approach to achieve high availability and confidentiality for data storage on multi-cloud," in Computer Software and Applications Conference Workshops (COMPSACW) 2013 IEEE 37th Annual. IEEE, 2013, pp. 212–217.

however, program level attacks will be undetectable. For instance, if data in a database is corrupted. That would be undetectable. Additional application-level authentication must be enforced in order to use TCCP.

2.6DATA PRIVACY PROTECTION METHODS

Anoymization is a technique that can be used. By hashing the unique identifiers of each row, a unique indexing[110] of each row in the database is created. The hashing information must be maintained locally, and the table must be separated by columns to separate cloud providers after these specific identifiers are removed. Person anonymity is preserved in this manner; but, since the whole column would be stored in a single cloud, data mining attacks may be used to anticipate valuable information.

2.7 LET'S SUM UP

This chapter reflects on the confidentiality and privacy of data collection and computation. Different approaches are compared, and issues and benefits of current methods are discussed. To deal with anonymization, authentication, data processing with separate operations, and secret stage, a hierarchical multi-cloud architecture with a shared pre-processing API and local database is proposed. By calling a generic API, the proposed architecture may include different authentication methods based on the data type and use, reducing complexity. However, there are a few issues with this design that need to be addressed: a) The call to the standard API will be resource intensive, necessitating caching and flexible procedures. b) Although the majority of computing and computation is performed in the cloud, some pre-processing and data-related information must be processed and managed locally. c) Since algorithms are used on encrypted data, customer-oriented algorithms must be created. Users must provide a thorough understanding of cryptographic files and a fully integrated framework benchmark must be developed, applied, and analyzed using quantitative and qualitative performance measures.

2.8FURTHER READING

- G. Ateniese, M. Steiner, and G. Tsudik ," Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," IEEE Trans. on Cloud Computing, 2015.
- Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou , "Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, vol . 25, issue. 1, 2014.

[110] A. Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp.612-613.

- D. Chen, and Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing,” IEEE International Conf. Computer Science and Electronics Engineering (ICCSEE), pp. 647-651, March. 2012.
- Dev, H., Sen, T., Basak, M. , Ali, M.E. “An Approach to Protect the Privacy of Cloud Data from Data Mining Based Attacks”, High Performance Computing, Networking, Storage and Analysis , pp. 1106 – 1115, 2012.
- X. Huang, X. Du, “Efficiently secure data privacy on hybrid cloud”, IEEE International Conference on Communications, pp. 1936-1940, 2013.

2.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the three layers of cloud computing platform?**

The cloud infrastructure architecture has three levels. Each physical computer has several virtual machines (VMs) built in the infrastructure layer. Customers are provided with a portal by the platform layer. Customers can have their own software, programs, and configurations installed. The cloud vendors provide the software stacks across the software layer.

2.10 ACTIVITY

Based on the role of data privacy and its integrity, explain how the breach if privacy can be protected and why is it necessary based on your opinion. (900-1000 words)

Unit 3: PRIVACY ISSUES AND DATA PROTECTION IN BIG DATA

3

Unit Structure

3.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- Impact of data security legislation on big data programs
- Privacy issues in big data analytics
- General Data Protection Regulation

3.2 INTRODUCTION

Big data refers to vast or diverse quantities of organized or unstructured data that can be used to provide value. Big data is typically described by a number of V-properties, such as length, velocity, and variety. Big data has now become a form of finance, with businesses vastly improving their processes and customer relations, and academics creating and enhancing science. Furthermore, the massive volume, rapid generation, and diversity of data necessitate unique storage and processing architectures.[111]

Although big data analytics has a lot of benefits, it also has a lot of privacy concerns when dealing with sensitive information. This is attributable to two elements of big data processing in particular. First, the more data there is, the more likely it is to re-identify people, often in databases that seem to lack personal linking knowledge. Second, big data research will infer new information from "harmless" personal data that is much more sensitive and was not meant to be disclosed by the individual affected.[112] A well-known example is a department store's study of purchasing habits in order to create personalized (targeted) ads, in which the algorithms accurately concluded that a young girl was pregnant. In other cases, such as medical care or testing, privacy risks can become much more severe.[113] A variety of technological means and legislation for privacy-preserving data collection have been introduced and developed in order to safeguard persons and their data.However, incorporating these techniques into a data processing system necessitates extra work during the design phase, and in many cases, such methods have an impact on the system's performance. As a result, companies and other organisations have not always been able to make this effort in the past, but this is changing as a result of recent privacy legislation and regulations.[114]

This unit discusses privacy challenges in big data processing and delves into two case studies that see how legitimate privacy standards can be fulfilled in big data and extremely sensitive personal data research ventures. Finally, it addresses the effects of the privacy-preserving approaches used on data collection and the outcomes.

[111] *NIST Big Data Public Working Group Definitions and Taxonomies Subgroup, "NIST Big Data Interoperability Framework: Volume 1, Definitions," National Institute of Standards and Technology, Tech. Rep. NIST SP 1500-1r1, Jun. 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1.pdf*

[112] *Gartner IT Glossary, "What Is Big Data?" 2018. [Online]. Available: https://www.gartner.com/it-glossary/big-data*

[113] *K. Hill, "How Target figured out a teen girl was pregnant before her father did," Forbes, Inc, 2012.*

[114] *J. T. Overpeck, G. A. Meehl, S. Bony, and D. R. Easterling, "Climate Data Challenges in the 21st Century," Science, vol. 331, no. 6018, pp. 700–702, Feb. 2011.*

3.3PRIVACY ISSUES IN BIG DATA ANALYTICS

A. Legal Regulations

From a legal standpoint, the EU General Data Protection Regulation (GDPR), which took effect in May 2018, is the subject of this article. If an organisation processes data of European residents, it is applicable to all organisations within the European Union (EU), the European Economic Area (EEA), as well as organizations from other countries. As a result, the GDPR affects the majority of large corporations around the globe.[115]

The GDPR governs how personal data is collected, stored, and processed. Any data that can be attributed to a single individual being is considered personal data. Which contains not just overt personal identification (such as full name and national ID number), but often indirect identifiers such as phone numbers, IP addresses, and photographs of recognizable individuals. Data without such identifiers is generally known as anonymous and falls outside the GDPR's domain (Recital 26).Big data analysis also yields observational conclusions with no causal connections to real people. As a result, processing only anonymous data is an easy way to comply with all GDPR specifications. The concept of anonymity, on the other hand, is not straightforward.[116]

Even if directly identifiable parameters are omitted from a dataset, combining the dataset with other information can allow single individuals to be re-identified. Background information assault is the term for this method of de-anonymization. The Netflix challenge in 2006 is a well-known case of re-identification. Netflix launched a dataset featuring 500,000 consumer movie reviews as part of a competition to discover more reliable movie recommendation approaches. Any personally identifiable information (PII) was excluded from the dataset, leaving only subscriber IDs (with no connection to the actual identity) and movie ratings (score, movie info, and date). However, researchers were able to classify particular consumers with a high likelihood by combining these data with other publicly available information (e.g., IMDB ratings).[117] Such well-known examples include identifying people based on their search words on the internet, anonymized DNA, and mobility info.

There are a variety of systematic metrics for determining a dataset's degree of anonymity (see next section). Since the GDPR does not have a clear or concrete concept of anonymity, it finds a dataset anonymous where re-identification is only possible through a great deal of difficulty or by impossible means. The GDPR establishes a set of legislative, bureaucratic, and technological standards for the collection of personal data, as well as various approaches. The most important concepts are outlined in this section. To begin with, in most instances, personal data collection is only permitted if the data subject has given his or her permission (Article 6).Exceptions occur when data collection is expressly permitted by statute or policy,

[115] *V. Marx, "Biology: The big challenges of big data," Jun. 2013. [Online]. Available: https://www.nature.com/articles/498255a*

[116] *M. Mostert, A. Bredenoord, M. Biesaart, and J. J. Delden, "Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach," European Journal of Human Genetics, vol. 24, no. 7, pp. 956–960, Jul. 2016. [Online]. Available: https://www.nature.com/articles/ejhg2015239*

[117] *A. Machanavajjhala, M. Venkitasubramaniam, D. Kifer, and J. Gehrke, "L-Diversity: Privacy Beyond k-Anonymity," in 22nd International Conference on Data Engineering (ICDE'06)(ICDE), 2006, p. 24. [Online]. Available: doi.ieeecomputersociety.org/10.1109/ICDE.2006.1*

or when it protects the data subject's "vital interests." Furthermore, approval must be limited to a single reason for data collection (Article 5). The data controller (the person in charge of gathering the data) cannot identify a too broad data collection function or alter it later on at will. Another data management theory is data minimization (Article 5), which refers to restricting personal data collection, storage, and use to data that are valid, sufficient, and, most significantly, essential for the processing intent. It's worth noting that pseudonymization is listed as a data minimization technique.[118] Identifiable parameters are replaced by other (randomly) generated identifiers in pseudonymized data. This typically has little detrimental effect on the data mining process and can be done by the data controller prior to moving the data to the data processor.

The data controller, which contains the mapping (also known as a pseudo-lookup table) pseudonyms to the recognizable parameters, can be used to relate the data processing performance. Aside from anonymized data, storage at the data controller must comply with the GDPR by using strategies that encrypt data in transit. Furthermore, Article 32 of the GDPR mandates the use of "effective technological and operational steps to ensure a degree of security appropriate to the danger," which generally entails the use of data encryption, access management, physical security, and (once again) pseudonymization.[119]

The storage restriction theory is an extension of the data minimization principle, which limits the length of data storage to a given (necessary) time. In the sense of data collection, it is also worth noting that automated decision-making procedures that have an effect on persons (Article 22), as well as the processing of highly sensitive data, such as biometric data (Article 9), need the data subject's "explicit" permission.

The GDPR does not explicitly answer the words "big data" or "data mining." Big data and the GDPR, on the other hand, are not always compatible, as the above definition shows. Big data mining, for example, focuses on the processing of vast volumes of data, which also goes against the data minimization concept. Furthermore, once the data has been compiled, new ideas for research are often introduced in data processing. The data subjects from whom the data were gathered, on the other hand, had originally given their permission for a different reason. As a result, from a legal standpoint, data collection should be performed on anonymized data wherever possible; otherwise, careful caution must be taken to ensure that the GDPR is followed. This could necessitate a data protection impact assessment (DPIA), which is a privacy-related impact assessment whose aim is to identify and analyze how certain acts or practices may affect data privacy (Article 35).

B. Technical Aspects

Technical means must be used to implement the legal specifications presented in the previous section. This segment discusses several privacy-preserving data mining techniques. The works of Agrawal and Skrikant, as well as Lindell and Pinkas, are well-known early approaches in this field.

[118] *D. Kifer and A. Machanavajjhala, "No free lunch in data privacy," in Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data, ser. SIGMOD '11. New York, NY, USA: ACM, 2011, pp. 193–204. [Online]. Available: http://doi.acm.org/10.1145/1989323.1989345*

[119] *A. Narayanan and V. Shmatikov, "Robust De-anonymization of Large Sparse Datasets," in 2008 IEEE Symposium on Security and Privacy (sp 2008), May 2008, pp. 111–125.*

In the first, data was distorted to make it anonymous, and then the anonymized data was subjected to a special decision tree classification analysis. In the second, the data was divided into two different datasets (a process known as pseudonymization), and a special multi-party computing algorithm was created to analyze the dataset.[120] This diagram depicts the common components of privacy-preserving data analysis: anonymization (as powerful as possible; at the very least pseudonymization) and possibly mining algorithms tailored to this type of updated data.

The attributes in a dataset are normally divided into four groups to aid in the anonymization process:

- Explicit identifiers: features that can be linked to a certain person, such as a social security number or an email address.
- Quasi-identifiers: attributes that do not explicitly connect an entity, but when the meanings of several attributes are merged, they will re-identify the person. Date of birth, ZIP code, and occupation are some examples.
- Sensitive data: features representing material that the data subject does not want exposed or, at the very least, not related to its identity. Diseases, financial situations, sexual identity, and current employment are some examples.
- Non-sensitive data: characteristics that do not fit into any of the previous categories (e.g., weather data).[121]

Unfortunately, this classification is not always clear: a (rare) disorder may also be used to classify a human. There are significant variations between the groups as well: the place of residence as a quasi-identifier may apply to millions of citizens in a big city, but just a few persons in small villages. A variety of anonymity models exist to measure the rate of anonymity and hence the threat of re-identification.

It is true that confidential knowledge is always of great importance to data miners, but also to adversaries. If the purpose of an analysis is to attach explicit identifiers to sensitive data, anonymization is clearly impossible, and the GDPR must be considered. In the very least, pseudonymization should be included in this situation. Data mining, on the other hand, is often used to find relations between quasi-identifiers and critical attributes, allowing data to be anonymized. Common anonymization methods are:

- Suppression: eliminating the values of an attribute entirely or replacing them with a dummy value (typically an asterisk "*") is a popular anonymization process. Explicit identifiers are commonly used for this operation.
- Generalization: within the attribute taxonomy, replacing attributes with more generic or abstract values, such as date of birth age (in years); age (in years)

[120] *J. Bohannon, "Genealogy Databases Enable Naming of Anonymous DNA Donors," Science, vol. 339, no. 6117, pp. 262–262, Jan. 2013.*

[121] *T. Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," Seton Hall L. Rev., vol. 47, p. 995, 2016.*

a number of years; ZIP code first two digits Normally, this operation is performed on quasi-identifiers.

- Permutation: grouping the data and shuffle- fling the sensitive values within each section. As a result, the link between quasi-identifiers and sensitive data is broken.
- Perturbation: replacing values in such a way that the original data is no longer connected, but the mathematical properties remain the same. Adding noise is a popular technique for perturbation.[122]

The presented models and anonymization methods are not only academically interesting, but they are also used in realistic privacy guidance (e.g., the Norwegian data protection authority). The foregoing anonymization operations undoubtedly result in the lack of metadata and a reduction in the data's utility. One may compare various anonymization methods to find the trade-off between privacy and utility using the utility and confidentiality metrics.

Mining anonymized databases often necessitates the use of specifically tailored mining algorithms. Decision trees, Bayesian classification, support vector machines (SVM), and stable multi-party computation are examples of classification and clustering algorithms that have privacy-preserving variants.

3.4 LET'S SUM UP

This chapter discussed the impact of data security legislation on big data programs and examined how privacy-preserving approaches can be implemented using two case studies. The outcomes were strikingly different. Participants in one study were asked to contribute to the collection and processing of biometric data in order to alleviate privacy issues. Furthermore, there were no issues during the data processing process. Data from an internal data base was included in the second project. Many data fields had to be anonymized, which made data processing more difficult and, in many cases, restricted. It is important to note that for programs and applications that deal with sensitive data, a data security impact review should be carried out at the very beginning of the project to recognise possible privacy issues and to adapt the research methodology to take privacy-preserving strategies into account.

3.5FURTHER READING

- J. T. Overpeck, G. A. Meehl, S. Bony, and D. R. Easterling, "Climate Data Challenges in the 21st Century," Science, vol. 331, no. 6018, pp. 700–702, Feb. 2011.

[122] *R. Agrawal and R. Srikant, "Privacy-preserving Data Mining," in Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, ser. SIGMOD '00. New York, NY, USA: ACM, 2000, pp. 439–450. [Online]. Available: http://doi.acm.org/10.1145/342009.335438*

- T. Z. Zarsky, “Incompatible: The GDPR in the Age of Big Data,” Seton Hall L. Rev., vol. 47, p. 995, 2016.
- A. Narayanan and V. Shmatikov, “Robust De-anonymization of Large Sparse Datasets,” in 2008 IEEE Symposium on Security and Privacy (sp 2008), May 2008, pp. 111–125.

3.6CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is covered under GDPR?**

The GDPR governs how personal data is collected, stored, and processed. Any data that can be attributed to a single individual being is considered personal data. Which contains not just overt personal identification (such as full name and national ID number), but often indirect identifiers such as phone numbers, IP addresses, and photographs of recognizable individuals.

3.7 ACTIVITY

Analyse through case studies the privacy issues and the application of GDPR. (900-1000 words)

Unit 4: PRIVACY AND DATA PROTECTION LAWS IN INDIA

4

Unit Structure

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- Data protection under the Indian Constitution
- Data Protection and Information Technology Act
- Data protection and corporate affairs

4.2 INTRODUCTION

In the international and national spheres, rights, which are intrinsic and inalienable characteristics of human society, have been reduced to a tangible and implementable text. Certain rights are stated explicitly in such texts, while others are introduced by an interpretative tool due to their integral relationship with other rights. One of the most significant and legitimate personal rights is the right to privacy. Person snooping from others gains influence as a result of it. The Universal Declaration on Human Rights, International Covenants on Civil and Political Rights, and the Convention on the Rights of the Child all mention the right to privacy.[123]

The right to privacy is one of the most important aspects of human life. This right has been described in India as an intrinsic part of the right to life and liberty, as well as the right to freedom of expression. A citizen is entitled to a "personal domain" that is free of unjustified state or third-party control or surveillance. Despite widespread awareness of the duty to respect privacy, universal human rights security systems are yet to adequately develop the precise content of this right. The lack of a consistent statement of the substance of this right has made its implementation and compliance more complex.

Since the right to privacy is a qualifying right, interpreting it poses difficulties in determining how the private domain is organized and defining conceptions of what constitutes public interest. The right of a human being has been encroached upon as a matter of general concern by the means of communication. Individuals should share knowledge and ideas in a room that is beyond the control of other members of society, the private sector, and potentially the State itself, according to the study of privacy of communications. Individuals should only use these protections to exercise their right to privacy in a communications scheme. The documentation of a right relating to non-interference with one's personal life occurred in the mid-nineteenth century. Through the commodification of technology, it has gained meaning. Any aspect of human life has been impacted by technology. The intrusion of modern technologies into human culture has been a daily occurrence.[124] It occurs either as a result of voluntary disclosure or as a result of unintentional knowledge collection. Demands for strict guidelines regulating the gathering and storage of personal information arose as a result of the monitoring capacity of powerful computer systems. The origins of contemporary laws in this field can be traced back to the first data security statute in the world, which was based on individual privacy. Data security is a form of privacy that has become a global phenomenon in recent years.

[123] Ghosh, Dr.Jayanta& Shankar, Uday. (2016). 'Privacy and Data Protection Laws in India: A Right-Based Analysis.

[124] Prakash Shah, "International human Rights: A perspective from India," Fordham International Law Journal, Vol. 21, Issue 1, Article 3, (1997): 24- 38.

The concept of defining data privacy as a civil right is a novel one. If a person has the right to privacy, he or she also has the right to data protection. Even with the current technical advancements, data security is also an emerging area.[125]

4.3CONSTITUTIONAL STATUS

There are some clauses in India's constitution which include "Freedom of Speech and Expression" and "Right to Life and Personal Liberty." The right to privacy as a human right is affected by these provisions. There have since been a variety of occasions where the right to privacy has been established as a constitutional right. This proposition's conceptuality is often linked to the current dimension of "Data Protection." The relationship between privacy and data security is inextricably linked. The right to data privacy is inextricably linked to an individual's "data."The analysis of constitutional provisions in order to comprehend the relationship between privacy and specifically scripted rights, as well as the explanation given by the country's highest court.[126] It looks at how various laws cope with the problem of data security. Finally, it makes a case for approaching data privacy issues from a rights-based perspective. "Human rights are rights enjoyed by all human beings at all times and in all places, purely by virtue of their humanity," Sir John Simmons says of human rights. Universality, freedom from social or legal recognition, naturalness, inalienability from social or legal recognition, naturalness, inalienability, non-forfeit ability, and imprescriptibility may be among their properties. An account of human rights can only be interpreted in this manner if it captures the central concept of rights that can be asserted by any human being at any time."

As a result, the principle of protecting civil rights also includes data security. For a person, the universality and freedom of data security are critical considerations. The right to privacy is therefore protected as a result of data security.[127] The most important and illuminating point is that privacy and data security are not mutually exclusive. These connections or shadows represent various fields that are interconnected with this regime. Privacy, like seclusion, solitude, and loneliness, is a concept similar to seclusion, solitude, and isolation, though it is not associated with these terms; it goes far beyond the strictly abstract facets of privacy, such as detachment from the business, fascination, and others' power, meaning the right to exclusive control of access to individual realms. The court's advocacy as a pathfinder of this developmental right is now being emphasized as a matter of right. Human rights should be acquired naturally, so the right of privacy must be acquired naturally as well.[128]

4.4ANALYSIS OF THE RIGHT BASED APPROACH

Only by various legislations will the right-based solution to the "data privacy" problem be scrutinized. The aim of this approach is to examine India's "data security" regime

[125] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, Vol. 4, No. 5 (1890): 193-220.

[126] Article 21 & 19 (1)(a) of the Indian Constitution, See also Udai Raj Rai, Fundamental Rights and their enforcement, PHI Learning Private Limited, New Delhi, (2011) p.19. See also Kharak Singh v. The State of U.P. and Ors. AIR 1963 SC 1295

[127] S.K. Sharma, Privacy Law: A Comparative Study (Atlantic Publishers & Distributors: 1994).

[128] Austin, Lisa Michelle, "Privacy law and the question of technology." Ph.D. Thesis, University of Toronto; 2005, ProQuest Dissertations and Theses.

from a global perspective. The topic of data security has gained a lot of traction in recent years, thanks to the growth of internet-enabled services, and has resulted in a surge in data collection, business process outsourcing, call-center services, accounting functions, and other corporate activities being outsourced.[129]However, as technology advances, so does the need to address the progress of legislation. As a result, data security enquires into the extent to which individuals' and organizations' identities, details, and data are covered under Indian law, particularly the Indian Constitution.

The defense provided by the Indian Constitution is highlighted because it is the "basic and ultimate root" from which all other laws derive their authority and power. (1) Privacy rights of interested parties in physical and cyber space, which these three shall present for discussion of constitutional aspects concern. (2) Freedom of communication obligations under Article 19 (1) (a). (3) Article 21 mandates the right to information of the general public. It categorically discusses the right to privacy, the right to access, the right to know, and electronic government, as well as trade secrets, intellectual property, and other topics from various perspectives. This analysis was carried out in order to clarify the association of rights. Furthermore, there is no equilibrium between knowledge and data processes, which is another flaw in this job.

The terms "data security" and "right to privacy" are being increasingly interchangeable. The 'personal security' will only be achieved if the invasion of privacy is halted. In general, and informational privacy in particular, privacy regulation has always been inextricably tied to technical advancement. Warren and Brandeis lament the "instantaneous images and newspaper enterprise that have violated the sacred precincts of private and domestic life; and countless mechanical machines threaten to make good the prediction that "what is whispered in the wardrobe shall be declared from the house-tops" in their seminal 1890 essay "The Right to Privacy." This is where the issue of privacy began.[130]

This is now being developed in the field of 'data security.' The concept of 'Data Protection' has many facets. The many facets of data security as a right, such as the right to access to data banks, the right to verify their accuracy, the right to update and amend them, the right to the secrecy of personal data, and the right to allow their dissemination: both of these protections are now combined to form the modern right to privacy. As a result, as a right-based policy, the linkage between "Data Protection" and "Privacy" status is quite reasonable in this case.

The appellant in R Rajagopal v. State of Tamil Nadu was the editor, printer, and publisher of a Tamil weekly magazine published in Madras who requested an injunction prohibiting the State of Tamil Nadu from intervening with the legal publication of Auto Shankar's autobiography, which was based on public records. In this case, Jeevan Reddy, J reaffirmed that the right to privacy is implied in Article 21 of the Constitution's protection of life and liberty. The Court has reiterated that every resident of this country has the right to be left alone in order to protect their privacy. As a result, the issue of "personal security" is developed in its own way by the "right

[129] Lee A. Bygrave, "Privacy and Data Protection in an International Perspective," Stockholm Institute for Scandinavian Law, (2010).

[130] Nicholas D. Wells, PoorviChothani and James M. Thurman, Information Services, "Technology, and Data Protection," The International Lawyer, Vol. 44, No. 1, International Legal Developments Year in Review: 2009 (2010): 355-366

to privacy." In the same way, both ideas have been classified as a matter of right under the Indian Constitution.

4.5DATA PROTECTION & INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

The terms "data privacy" and "Information Technology Act" have different implications in comparison to each other. The Act's goals expressly state that the security of cyber-relationships is a priority.[131] It ensures the data from information networks is protected from any types of breaches. The said Act contains protections aimed at preventing the unauthorized usage of servers, information networks, and data stored on them. Several clauses relating to "data security" have been added to the bill. The updated sections 43A and 72A of the Act talk specifically to data security. This 2008 Amendment Act is a major move forward in the fight against the plethora of cybercrime. The reforms in Indian legislation on constitutional data security have finally yielded to the demands of the United States and European nations over the last decade. The service provider is now serving jail time for violating a contractual requirement by disclosing "sensitive knowledge." Furthermore, revealing "private personal details" leaves the victim responsible for damages.[132]
As a result, privacy security has been granted the same position as a matter of right. The key emphasis given to analyze the EU Data Protection legislation and the stands of the Indian Information Technology Amendment Act 2008 is technical growth. In terms of the Information Technology Act 2008, it discusses the corporate use of data such as waste, share, discloser, publication protection measures, and penalties. Another example is the IT Rules 2011, which gives the appearance of presumption of right interest in its clauses. The significance of India's outsourcing industry and how it can affect the flow of business from European Union firms. This essay also discusses the newly notified legislation pertaining to the security of confidential personal data, as well as the Indian regulations, comparing their requirements with the UK Data Protection Act 1998 at times. As a result, the primary right-based approach to human privacy security is claimed.

4.6DATA PROTECTION & CORPORATE AFFAIRS

The alliance between "data privacy" and "corporate affairs" is now forming a right-base strategy. The business world is seriously impacted in a variety of ways. The importance of data entry, disclosure, sharing, and processing cannot be overstated. In the business world, data processor or data manager custody has played a critical part.[133] It is sometimes the duty of a private company to share or not to share information. This is where private and charitable organizations clash with law enforcement agencies. When someone tries to view details or place an order for a product, the ad online will prompt them to fill out a form.

[131] Bygrave, L.A., "Data Protection Law: Approaching Its Rationale, Logic and Limits," Kluwer Law International, The Hague / London / New York (2002).

[132] Justice A P Shah Committee Report, "Report of the Group of Experts on Privacy", (2012), Accessed October 21, 2016, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

[133] H L A Hart, "Are There Any Natural Rights?" The Philosophical Review Vol 64, NO 2 (1955): 175-191,

Now the question is whether the data retained by the authority after application of this information complies with public policy. In terms of this, in the banking industry, the banker has a responsibility not to reveal information in their hands, resulting in a violation of the client's duty of privacy and confidentiality. The extent of a banking customer's right to privacy was limited because it interfered with the right to access and public information. The Securities and Exchange Board of India Act (1992) established the Securities and Exchange Board of India (SEBI) to control and regulate the use of people's credit records. The government's reactive control is mediated by the Security Exchange Board of India, which is given limited access to private-sector data relating to the stock market under the Act. As a safeguard against unauthorized reactive access, SEBI is only allowed to inspect if it has reasonable grounds to believe that: a company has engaged in insider trading or fraudulent, unfair trading practices have been used, securities transactions have been handled in a way that is detrimental to the investor,[134] or an intermediary or any person associated with the securities mafia has been involved in insider trading or fraudulent, unfair trading practices have been used, or an intermediary or any person associated with the securities market is contravening any provision in the Act.

By penalizing someone who fails to have the necessary information, the Act reinforces reactive access to and dissemination of information. The Credit Information Companies Regulation Act, 2005 ("CICRA") mandates that credit information belonging to persons in India be obtained in accordance with the CICRA regulation's privacy standards. Entities responsible for processing and storing the data have been held accountable for any potential data exposure or modification. The CICRA also established a stringent system for details relating to credit and finances of individuals and businesses based on the Fair Credit Reporting Act and the Graham Leach Bliley Act.[135]

The Reserve Bank of India recently informed the CICRA Regulations, which establish strict data privacy principles. As a result, the fields of "data security" and "corporate relations" are moving in the same direction as the "right-based solution."

4.7 LET'S SUM UP

Data security has been viewed as a right from various perspectives, according to the study of various themes. All of the subjects, such as the right to privacy, the right to records, information security, and corporate relations, were emphasizing the importance of accepting data security as a right. In this age of technical liberalization, the aim of the issue is to reinforce the view of data privacy as a right. The reach of technology is expanding all the time, and in order to keep up with this trend, the data privacy regime must be strengthened in order to safeguard individual liberty. The aim of this chapter is to define the right to privacy and data security as a constitutional right that is warranted to regard as such after study. Only the entire legal provision as a right to data privacy will satisfy others' intrusion and infringement of individual liberties. Data security can take on a universal approach depending on the institutional standing. To grant data protection a special status as a right, the various

[134] Dr. Amit Ludri, Law on protection of personal & official information in India, The Bright Law house, New Delhi, 1st Edition, (2010).

[135] Praveen Dalal, "Data Protection laws in India: A Constitutional Perspective," Accessed October 21, 2016, http://ipmall.info/hosted_resources/gin/PDalal_DATA-PROTECTION-LAW-ININDIA.pdf.

aspects of data protection, such as data collection, transmission, storage, confidentiality, and access, should be brought together in a legal context. Knowledge of the proper foundation approach to data security and privacy must be universally distributed.

4.8FURTHER READING

- Dan Jerker B. Svantesson, "Systematic Government Access to Private Sector Data in Australia," 2/4 International Data Privacy Law, (2012).
- Denis O'Brien, "The Right of Privacy," Columbia Law Review, Vol. 2, No. 7 (1902): 437-448.
- Daniel J. Solove & Paul M. Schwartz, "Privacy, Information and Technology," Wolter Kluwer Law & Business Publisher in New York, (2011), 79-256.
- M. M S Karki, "Personal Data Privacy & Intellectual Property," Journal of Intellectual Property Rights, Vol 10. (2005): 59-63

4.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are special and general rights?**

Special rights are derived from 'special transactions [or] particular relationships,' such as commitments, contracts, or political association membership, while general rights are derived from 'all men capable of choice...in the absence of those special circumstances which give rise to special rights.'

4.10 ACTIVITY

Based on the data protection laws discussed in the chapter, critically analyse the implementation of such laws and recommend solutions to the same, if any. (900-1000 words)

Block-4

INTERNATIONAL LAW ON DIGITAL RIGHTS

Unit 1: INTERNATIONAL LAW ON CYBER SECURITY IN THE AGE OF DIGITAL SOVEREIGNTY

1

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- human rights perspective of cyber governance
- fundamental freedoms in digital space

1.2 INTRODUCTION

Through the use of cyber technologies such as the Internet and mobile devices, good cyber governance must create a human rights-based strategy for (1) more openness, (2) more openness, and (3) more stakeholder involvement. Furthermore, good cyber governance promotes and protects human rights through technology. Cyberspace, though, is a borderless public space in which people, regardless of their citizenship, race, sex, political affiliation, or gender collaborate and connect.[136] Cyberspace and the Internet are used by individuals to perform business, make policy, and organize their personal lives. Yet this space does not have any common rules or standards, a governance apparatus, or enforcement or control mechanisms that would protect and foster people's activities. Universal human rights principles and guidelines will act as guides and benchmarks for setting up governance systems in cyberspace. Cyberspace, thanks to emerging technology, provides an arena with a large number of people that can impact and manipulate one another. This room is clear and impartial by default, but the people who use it often identify, enlarge, restrict, or censor it. Internet correspondence is mostly private and used and exchanged with the public worldwide, who normally stays unknown to the actual Internet user; specifically, each of us. We nonetheless share our most sensitive and confidential data with this anonymous group.This modern, open society now has between 2 and 7 billion Internet users. If cyberspace were a nation, it would be the largest and most populous in the world, although one without any constitutions or government. There are no legislative or other political decision-making bodies in this "room."[137] It has no police or law enforcement system, let alone security mechanism to uphold human rights for all Internet users. Therefore it can be argued that (i) cyber governance does not need new human rights norms or standards, but rather new governing and monitoring regimes and enforcement mechanisms that guarantee and safeguard the human rights of all people who use cyberspace; (2) we need to identify all private, public, governmental, and international actorswho carry responsibilities in either violating or fostering human rights in the Internet; and (3) all users need to establish mechanisms that enhance trust in institutions (e.g., governments), companies (e.g., Internet providers, servers), and organizations (e.g., Facebook, YouTube).[138]

1.3CYBER GOVERNANCE AND HUMAN RIGHTS

[136] Eugen, Petac&Petruţ, Duma. (2019). Exploring the New Era of Cybersecurity Governance. AnaleleUniversitatiiOvidius Constanta. XVIII. 358-363.

[137] Aitel, D. (2013). Cybersecurity essentials for electric operators. The Electricity Journal, 26(1), 52-58.

[138] Allen, J. Governing for Enterprise Security. Pittsburgh: Carnegie Mellon University, 2005. Available on:

On one hand, the Internet and cyberspace can foster and enhance individuals' inclusive participation and access to politics and business, which they otherwise would not have. On the other hand, it can also exclude those who are Internet-illiterate or have difficulty accessing the Internet (e.g., children, aging people, and people without Internet-access). Billions of Internet users have now developed anonymous twin-identities in this new space by exchanging private information in cyberspace, without ever getting the opportunity to erase the information. Personal relationships and friendships established via social media platforms such as Renren and Facebook will seem to be private while revealing a wealth of personal information; as a result, it is a space for public privacy.[139]Anyone with access to this infinite room can now deal with businesses and companies, schooling and training, investments and economics, private communications, and even health and personal matters. Finally, a strong cyber governance system is absent in cyberspace: a quasi-government or governance regime that oversees the interests and claims of its people through oversight and compliance bodies.Although international governmental organizations (IGOs) such as the United Nations (UN), the Organization of American States (OAS), the African Union (AU), and the European Union (EU) aim to establish international standards and legally-binding treaties for the use of cyberspace and the Internet, they frequently fail to do so. Since their mandate to uphold human rights is entirely dependent on state authority and governments, each state's powers and compliance capacity always stop at state boundaries.

Also, IGOs and international courts often have limited measures and means to protect human rights, let alone enforce them.Since cyberspace has no physical or national boundaries, the methods for governing this current borderless regime are still being developed. Human rights norms and principles, such as the right to privacy, protection, health, free speech, movement, and industry, offer guidelines to the various players engaged in the regulatory design of the cyberspace regime in the debate and attempt to set up a cyberspace governance regime. If established, the cyberspace governing body will consist of multiple stakeholders and actors. This includes national,international, as well as private actors such as representatives of companies, social networks, NGOs, and individuals. The World Internet Governance Forum under the UN has initiated such a concept.

1.4DIGITAL SPACE AND FUNDAMENTAL FREEDOMS

Other basic freedoms and privacy human rights addressed in this context include freedom of speech, faith, political thought, poetry, and written texts; free and fair access to information; and the security of personal information such as family relationships, associations, and health information.[140] Furthermore, protected privacy from abuse and persecution on the Internet based on one's own political, ethical, or gender status, as well as undisclosed personal, educational, or health records, is a

[139]Cebula, J. J., & Young, L. R. (2010). A Taxonomy of Operational Cyber Security Risks, Software Engineering Institute. Available at: .

[140]Chinn, D., Kaplan, J. and Weinberg, A., 2014. Risk and responsibility in a hyperconnected world: Implications for enterprises, Report - January 2014. [online] Geneva: Word Economic Forum. Available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/risk-andresponsibility-in-a-hyperconnected-world-implications-for-enterprises

cornerstone of human rights in cyberspace. Cyber human rights should protect an individual's intellectual property and creativity in areas such as art, movies, pictures, literature, scientific results, etc. with access at any time to fair and open trials. Good cyber governance has to be conducted over a domain of an individual's public privacy, which includes public and private data. It must strike a balance between Internet freedom of information and expression and the security and privacy of individuals in cyberspace. Privacy, according to international principles and concepts, is a personal space where we can confidently and freely grow our personalities, exercise our talents and abilities, protect our fitness, and enjoy social interactions with family and friends.As a result, using the Internet as a service medium for private reasons without fear of third parties, such as governments or businesses (e.g., national security services, Google+, Microsoft), accessing, selling, or openly posting our data for national security or commercial purposes without our permission is referred to as privacy in cyberspace.

Maintaining public privacy eventually faces the task of balancing our personal, technical, and private interests while providing norms and laws that may hinder any degree of privacy using the Internet as a free and open access communication platform. The debates and discussions around Internet freedom and privacy rightsare fundamentally important in the areas of data protection, cybersecurity, cyber surveillance, and cyberwar through computer viruses. Some call it the "World Wide War" in which various state and non-state actors such as individual hackers are equally involved. Commercial-state or inter-govern- mental agreements, such as the Stop Online Piracy Act (SOPA), the NSA's surveillance program, PRISM, or the Anti- Counterfeiting Trade Agreement (ACTA), are just a few governmental initiatives to regain the control over the borderless dataflow.

The problem would be determining if these frameworks and commitments will fully protect human rights. The often declared 'right to Internet,' which aims to include individual access to the Internet at any time, and the right to be forgotten, which ensures that one's own personal data remains private and can be deleted at any time, are already part of overall human rights standards concerning access to information, privacy, and data protection (as in the EU Fundamental Rights Charter) and participation. The EU Court of Justice passed a land- mark decision in May 2014 that but- tresses privacy and the right of users to have their data removed or forgotten from the Internet. The ruling targets search engines and data providers such as Google, YouTube, and Facebook. Unfortunately, it only applies to the EU territorial space. A global solution has yet to come.[141]

The European Court of Human Rights' Research Division made some progress in 2011 by releasing a landmark paper on future case law surrounding Internet-related privacy and retention problems. Other foreign or domestic courts, on the other hand, can take some time to interpret the legal rights established by the EU Court of Justice. Human rights are often inscribed and enforced by treaties, customary international law, general principles, and other sources of international law. Governments, corporations, persons, and other lawful bodies (duty bearers) have rights and responsibilities to behave in certain ways or refrain from certain actions. There is no hierarchy of human rights, which are sometimes referred to as social, legal, economic, political, or cultural rights. Without one another, these various types of human rights cannot be practiced or enjoyed.For example, the universal right to

[141] Proença, D., Vieira, R. and Borbinha, J., 2016. "A maturity model for information governance". In: International Conference on Theory and Practice of Digital Libraries. Cham: Springer, pp. 15-26.

access exists only where the information does not infringe on the integrity or privacy of others. This is the Golden Rule-based holistic approach to human rights: “Do not hurt others in the way that you may not want done to you.”In this vein, a cyber human rights regime should be calibrated and assessed insofar that it would not infringe on others’ rights.

That being said, protection of data should never justify censorship or random surveillance of individuals. Finding the balance depends very much on who decides the limits and borders of freedom of information. The greater the number of parties involved, the more likely the final balance would be agreed. Finally, in 2012, the United Nations Human Rights Council told us that human rights are applicable both online and offline, and that whether they are broken in cyberspace or in physical space across borders makes no difference. However, the issue of who is the duty bearer remains unanswered. Who will defend, execute, and uphold human rights in cyberspace if government authorities stop at state borders? In 3013, the issues of cyber espionage and misuse of private data came about through the NSA affair between the United States, Germany, and Brazil. The former NSA contractor, Edward Snowden, revealed the U.S. government’s warrantless and limitless surveillance of U.S. citizens and Internet users around the world.

The United States is now charging Snowden under the U.S. Espionage Act, but Snowden remains in exile in Russia while theU.S. government works on extradition. Snowden’ s revelations continue to strongly impact the debate about privacy and its insufficient legal development and heavily violated laws. Even though the UN, the EU, and many nations extensively fine-tuned their laws and regulations on data protection in 2013, the main issue remains unresolved: how can privacy and freedom rights be safeguarded in cyberspace, if at all? Individually, many users started to adapt and become more cautious.[142] Consequently, self- censorship by users could not be avoided and manysensitive communications no longer take place online. Facebook users have become alarmed at posting private pictures online, and millions of users no longer send their e-mails unencrypted. The need for technical tools such as encryption and deciphering technology are highly demanded. In Europe alone, the number of encrypted data transferred rose in 2014 from 1.5% to 6.0%. Yet overall Snowden’s revelations demonstrated that the problems of global surveillance - conducted by most NSAs in this world - need global answers, not just national or regional ones, let alone technical ones. The many national laws passed over the past year regarding data protection can only create more time, but not deliver the solution. Meanwhile, private, governmental and non governmental actors have to discuss and decide which will be the common cyber- rules, standards and governance mechanisms that will end anarchy in cyberspace in the near future. In response to these and other revelations, the UN Special Rapporteur on Freedom of Expression Frank de la Rue highlighted the fact that privacy and freedom of expression are interlinked and mutually dependent.

As a result, without adequate legislation and legal standards to ensure the privacy, security, and anonymity of communications journalists, human rights defenders, and whistleblowers, it is impossible to ensure that their communications will not be subject to states’ security uses.” Jon Perry Barlow wrote the “Declaration in

[142]Sonmez, M. and Yildırım, S., 2015. “A Theoretical Aspect on Corporate Governance and Its Fundamental Problems: Is It a Cure or Another Problem in the Financial Markets?”. Journal of Business Law and Ethics, [online] Volume 3 (No. 1 & 2), pp. 20-35. Available at: http://jblenet.com/journals/jble/Vol_3_No_1_June_ 2015/2.pdf

Independence of Cyberspace” in 1996, describing the situations and controversies that today’s Internet users are concerned with around the world.Barlow realized twenty years ago that the Internet world, and therefore the global consumer community, needed to create their own social contracts and figure out how to deal with their challenges based on the Golden Rule, which is the basis for realizing human rights. Whether or not such cyberspace social contracts are ever implemented, the concept underlying them is personal responsibility and commitment to human rights, which we, as members of the global community (private or public), have long subscribed to. So-called ‘digital rights’ are already embedded in freedom rights, such as those stated in the Universal Declaration on Human Rights (UDHR) or the International Covenant on Civil and Political Rights (ICCPR). These rights allow the access and use of information and communications technology, like computers and digital media, to enhance any of the aforementioned human rights and the overall human right to information.[143] As a result, on December 10, 2013, the 65th anniversary of the UN’s proclamation of the Universal Declaration of Human Rights, over 500 authors and Nobel Laureates signed a petition asking the UN to draft an international bill on digital rights. The user community’s overwhelming enthusiasm for such a proposal is anticipated to have an effect on the advancement of global Internet governance concepts.

1.5 LET’S SUM UP

Governance, ultimately, human rights -oriented cyber governance is a new trend in which global Internet users aim to uphold their basic human rights through good cyber- governance principles. Yet there is no global rule of law culture in cyber-space as of yet, let alone any monitoring or enforcement mechanism based on the multi-stakeholder approach that would safeguard the rights of development towards an open and fair cyber governance regime.

1.6FURTHER READING

- A. Mihr (2013) Public Privacy-Human Rights in Cyberspace, Working Paper, Utrecht University.
- MindaugasKiskis (2011) Entrepreneurship in Cyberspace: What do we know?, Social Technologies, MykolasRomeris University, I (i), 37~4
- Internet Governance Forum Helen Nissenbaum, “Toward an Approach to Privacy in Public: Challenges of Information Technology (1997) 7 (3)» Ethics & Behavior, 207-219.
- Court of Justice of the European Union (May 2014), Factsheet about Right to be Forgotten ruling C 131/12 .

[143] ITU, 2008. Overview of cybersecurity, ITU-T X.1205. [online] Available at: https://www.itu.int/rec/T-REC-X. 1205-200804-I/en

1.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Why is Human-based rights approach needed for Good Cyber Governance?

Through the use of cyber technologies such as the Internet and mobile devices, good cyber governance must create a human rights-based strategy for (1) more openness, (2) more openness, and (3) more stakeholder involvement. Furthermore, good cyber governance promotes and protects human rights through technology. Cyberspace, though, is a borderless public space in which people, regardless of their citizenship, race, sex, political affiliation, or gender collaborate and connect.

1.8ACTIVITY

Elaborate the fundamental freedoms in digital space which should be protected. (800-900 words)

Unit 2: PRIVACY AND DATA PROTECTION: AN INTERNATIONAL PERSPECTIVE

2

Unit Structure

2.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- privacy provisions of various countries
- data protection of the individuals
- data protection and privacy

2.2 INTRODUCITON

This chapter examines the establishment of legislative instruments (statutes, recommendations, guidance, and so on) to protect privacy and related interests in the collection of personal data across jurisdictions.In Europe, such instruments are commonly referred to as "data security" instruments, which is also the nomenclature used in this chapter. Defense of "privacy," "personal privacy," or "information privacy" is the preferred nomenclature outside of Europe. Regardless of these terminological distinctions, all of the instruments constituting the subject of this chapter are expressly aimed at restricting the collection of data relating to, and promoting recognition of, individuals (i.e., personal data) in order to preserve, at least partially, the privacy and related interests of those persons.[144]

The central rules that are applied to the processing of such data herein embody a set of mostly procedural, "fair information" principles stipulating, among other things, the manner and purposes of data processing, measures to ensure adequate data quality, and measures to ensure that the processing is transparent to, and influenced by, the individual to whom the data relate ("data s"). These instruments, when taken together, constitute an area of law and policy that has grown in sophistication, spread, and normative significance over the last four decades.[145]About forty countries have already adopted data privacy legislation that is reasonably robust. A vast variety of international agreements supplement and also inspire these national programs. An enormous body of scholarly commentary envelops the regulatory sector, analyzing privacy and data security topics from a range of viewpoints. As a result, the global data security landscape is extremely complex, and it is beyond the reach of this chapter to adequately represent all of its nooks and crannies.

2.3CONCEPTUALISATIONS OF PRIVACY AND RELATED INTERESTS

Privacy is a hot topic of discussions regarding the social and political dangers raised by new information and communications technologies (ICT). This is especially true in the United States of America (USA), where the term "privacy" is commonly used in cultural, scholarly, and legal debate. When significant debate began in the 1960s over the effects of computerized collection of personal records, the word "privacy" was coined as a catch-all term for the slew of concerns posed by the (mis)use of

[144] See generally Regan, P.M., Legislating Privacy: Technology, Social Values, and Public Policy, University of North Carolina Press, Chapel Hill / London 1995.

[145] See, e.g., Westin, A.F., Privacy and Freedom, Atheneum, New York 1970; Miller, A., The Assault on Privacy: Computers, Data Banks and Dossiers, University of Michigan Press, Ann Arbor 1971.

machines. However, protection is not the only word that has been used in this way. Other, partially overlapping terms, such as “democracy,” “liberty,” and “autonomy,” have also been mentioned.[146] The debate in the United States, especially in the 1960s and early 1970s, about the privacy challenges faced by modern ICT had a significant impact on debates in other countries. “Almost every issue that arose in Europe was also an issue in the United States, but at a much earlier time and on a much larger scale,” writes Hondius.

The importance of the privacy principle in American discourse contributed to its popularity in other debates. This is most noticeable in English-speaking countries and international forums where English is used as a working language. And in countries where English is not the primary language, much of the same debate has been framed, at least at first, around definitions that are loosely equivalent to, or embrace, the principle of privacy.Nonetheless, the area of law and policy that arose from early European discussions about the privacy risks faced by ICT has often been defined using a nomenclature that avoids overt references to the words “privacy” and “privacy-related terms.” The expression “data security” is derived from the German word “Datenschutz.” While the nomenclature is flawed in many ways, including failing to indicate the core interests represented by the standards to which it is intended to refer, it has achieved widespread acceptance in Europe and, to a lesser degree, elsewhere. However, the word “data protection” is gradually being used in its place. The latter term is potentially more fitting than “data security” because it better communicates the core issue(s) at hand and serves as a link between North American and European policy debates.However, it would be a mistake to presume that the terms “data security” and “privacy” are interchangeable. They are not similar, at least from a European perspective, despite their close relationship. The term “data security” is usually used to refer to a collection of rules that cover a wider spectrum of concerns than just privacy. And the degree that such conventions address privacy rights, they only address the informational aspects of privacy rather than the spatial or physical dimensions.

Various countries and territories have their own terminological quirks, which are partially due to varying jurisprudential contexts for the debates in question.[147] The debate in Western Europe has often relied on the region’s jurisprudence on legal identity rights. As a result, the definitions of “Persönlichkeitsrecht” and “Persönlichkeitschutz” play a central role in German and Swiss data security debate. The principle of “personvern” (“protection of person(ality)”) dominates Norwegian discourse, while “integritetsskydd” (“protection of (personal) integrity”) dominates Swedish discourse.[148]Latin American debate in the region, on the other hand,

[146] See, e.g., United Kingdom, Committee on Privacy (the Younger Committee), Report of the Committee on Privacy, Cm. 5012, Her Majesty’s Stationery Office, London 1972; Canada, Department of Communications and Department of Justice, Privacy and Computers: A Report of a Task Force, Information Canada, Ottawa 1972; Australian Law Reform Commission, Privacy, Report no. 22, Australian Government Publishing Service, Canberra 1983; Morison, W.L., Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys-General, Report no. 170/1973, Australian Government Publishing Service, Canberra 1973.

[147] See, e.g., Hughes, G.L. and Jackson, M., Hughes on Data Protection in Australia, Law Book Co. Ltd., Sydney 2001, 2nd ed.

[148] See, e.g., Guadamuz, A., Habeas Data: The Latin American Response to Data Protection, The Journal of Information, Law and Technology 2000, no. 2, “www2.warwick.ac.uk/ fac/soc/law/elj/jilt/2000_2/guadamuz”; Organization of American States (O.A.S.), InterAmerican Juridical Committee (rapporteur Fried, J.T.), Right to Information: Access to and Protection of Information and Personal Data in Electronic Form, in Annual Report of the Inter-American Juridical Committee, CJI/doc. 45/00, p. 107 et seq. While the concept originates in South

continues to revolve around the definition of “habeas data” (roughly translated as “you should have the data”). Due-process doctrine, which is founded on the writ of habeas corpus, gives rise to this definition. Many of the definitions listed above are subject to definitional inconsistency. The most well-known example is “privacy.” Various meanings of the term abound, and a lengthy – yes, a lengthy – controversy has erupted, mostly in American circles, over which meaning is the most accurate. Parallel discussions on related concepts can be seen in other nations, but they tend to be somewhat less robust than the privacy debate. Any of the above controversy revolves around whether privacy should be classified as a state, a claim, or a privilege. Aside from that, the controversy exposes four major definitions of privacy. One collection of meanings is based on non-interference, while another is based on restricted access. A third group of concepts considers privacy to be the ownership of content.

A fourth set of meanings combines concepts from the other three sets, but only applies to private or important facets of people’s lives. Not unexpectedly, concepts of privacy in terms of information security are most common in discussions of data protection law and policy. Most of the debate, both in the United States and abroad, revolves around the concept of access management. However, in Europe, the term is not necessarily immediately connected to the concept of privacy; it is either linked to similar terms such as “personal dignity” (as in Swedish discourse) or it stands alone.The German concept of “information self-determination” (“informationelleSelbstbestimmung”), which is the substance of a constitutional right derived from a historic ruling by the German Federal Constitutional Court in 1983, is the most notable example of the above (Bundesverfassungsgericht). The concept, as well as the right attached to it, has had a significant effect on the advancement of data protection law and policy in Germany and, to a lesser degree, other European countries.Despite their widespread acceptance, concepts of knowledge ownership and self-determination have seldom been interpreted in terms of an individual “owning” information about himself or herself, so that he or she may be entitled to royalties for its use by others. Property rights doctrines, on the other hand, have rarely been championed as a desirable foundation for data protection rules. The few advocates of a property rights approach have appeared to come from the United States, but there has been some scattered activism internationally.[149]

2.4CONCEPTUALISATIONS OF THE VALUES SERVED BY PRIVACY

What are the ideals supported by respect for privacy as described by different nations or cultures? Is anonymity, for example, perceived as primarily (or exclusively) of importance to individuals or as having wider societal benefits? In the United States, much discussion of privacy and privacy protection focuses only on the benefits of people as individuals. Individuality, integrity, integrity, emotional freedom, self-evaluation, and inter-personal relationships of affection, friendship, and trust are usually cast in terms of securing (or helping to secure) individuality, autonomy,

America, it has also begun to gain a foothold in parts of South-East Asia. In 2008, the Supreme Court of the Philippines formally adopted a “Rule on the Writ of Habeas Data” as a Rule of Court.

[149] See, e.g., Warren, S.D. and Brandeis, L.D., The Right to Privacy, Harvard Law Review 1890, vol. 4, p. 193, 205 (arguing that the right to privacy in Anglo-American law is part and parcel of a right “to be let alone”).

dignity, emotional release, self-evaluation, and inter-personal relationships of love, friendship, and trust.[150] They are primarily about "achieving individual goals of self-realization," as Westin puts it.The flip side of this focus is that privacy and privacy protection are often seen as being in direct conflict with the interests of a larger "society." This viewpoint is often expressed in arguments that privacy rights are incompatible with social needs.

Casting the value of privacy in purely individualistic terms continues to be a prevalent feature of many other countries' equivalent debate. Indeed, it is a key component of what Bennett and Raab refer to as the "privacy model" – a series of liberal assumptions that guides the implementation of data security policy in the vast majority of advanced industrial countries. Despite this, the paradigm's hold ranges from country to country and culture to culture. When comparing the German Federal Constitutional Court's jurisprudence to that of US courts, the differences are clear.[151]The former emphasizes that the importance of data security norms is largely determined by their capacity to provide the requisite conditions for active citizen participation in public life; in other words, to ensure a healthy democracy. In American law, this viewpoint is underdeveloped. We're also seeing a growing awareness in intellectual debate on both sides of the Atlantic that privacy and data security norms are important not only for individuals, but also for the preservation of societal civility, pluralism, and democracy.

A related trend is the growing awareness by academics that data security laws represent a variety of needs, some of which go far beyond conventional notions of privacy. This understanding has probably progressed the most in Norwegian debate, which has established relatively sophisticated models of the different interests supported by data protection laws. Ensure sufficient quality of personal records, "citizen-friendly" government, proportionality of power, and the rule of law are among these interests.The realization that data security policies are about more than protecting privacy has spread beyond academia and into regulatory bodies in Norway. Indeed, in addition to the needs for anonymity and personal dignity, Norway's main law on the subject includes an objects provision expressly relating to the requirement for "adequate quality of personal knowledge." Any other European countries' equivalent regulations have objects provisions that cover more than just privacy.The French legislation expresses the broadest, if not the most audacious, set of goals: "Information technology should be at the service of every citizen." It will be established in the sense of international collaboration. It must not infringe on people's identities, rights, privacy, or personal or public liberties." Also notable is the explicit concern expressed in many German Länder' early data security laws for preserving State order based on the principle of division of powers, as well as

[150] Laudon, K.C., Markets and Privacy, Communications of the Association for Computing Machinery 1996, vol. 39, p. 92–104; Lessig, L., Code and Other Laws of Cyberspace, Basic Books, New York 1999, p. 159–162; Rule, J.B. and Hunter, L., Towards Property Rights in Personal Data, in Bennett, C.J. and Grant, R. (eds.), Visions of Privacy: Policy Choices for the Digital Age, University of Toronto Press, Toronto 1999, p. 168–181; Rule, J.B., Privacy in Peril, Oxford University Press, Oxford 2007, p. 196–198. Cf. Schwartz, P.M., Property, Privacy, and Personal Data, Harvard Law Review, 2004, vol. 117, p. 2056–2128 (critically discussing various objections to a property approach but ultimately arguing in favour of a qualified "propertization" of personal data).

[151] See, e.g., Blume, P., New Technologies and Human Rights: Data Protection, Privacy and the Information Society, Paper no. 67, Institute of Legal Science, Section B, University of Copenhagen 1998.

ensuring so-called “data equilibrium” (“Informationsgleichgewicht”) between the legislature and other State institutions.[152]This “equilibrium” applies to a situation in which the legislative is able to obtain information (personal and/or non-personal) that the executive has access to. In certain nations, however, there is some confusion about the rights and principles are promoted under data protection legislation. This is expressed in scholarly debate, in the fact that certain statutes lack objects clauses that formally define the specific objectives or principles that the statute is meant to represent, and in the frequently ambiguous manner in which modern objects clauses are drafted.[153]

2.5SOCIETAL AND CULTURAL SUPPORT FOR PRIVACY

Making fair assessments of the degree to which different nations or societies value privacy is challenging – a challenge that clearly extends to comparing the regulatory regimes for privacy and data security of different countries. This challenge stems in part from a lack of systematically collected scientific evidence, and in part from the fact that privacy concerns vary widely across countries and cultures.Proposals to introduce multi-purpose Personal Identification Number (P.I.N.) schemes similar to those in Scandinavia, for example, have traditionally been met with strong opposition in the United Kingdom (U.K.),[154] despite the fact that video surveillance of public places in the U.K. appears to be far more extensive than in Scandinavian countries, and indeed the rest of the world. The level of privacy varies greatly across nations and societies, as well as across long stretches of time.Furthermore, the ways in which people establish, protect, and improve their respective states of privacy, as well as the degree to which they express a preference for privacy, differ from culture to culture due to a variety of reasons. Around the same moment, the need for secrecy continues to be a universal human characteristic. Human beings seem to follow different techniques for cultivating other types of social distance including in communities where physical or spatial solitude appears to be restricted.[155]

If there is a panhuman desire for anonymity, it tends to be embedded in social rather than physiological or biological considerations. According to Moore, the desire for privacy is primarily a social construct. Moore’s groundbreaking study suggests that an extensive, deeply established respect for privacy is only possible in a comparatively dynamic society with a firmly felt distinction between a domestic private domain and public sphere “privacy is limited where technology and social organisation are restricted”. However, technical and corporate considerations aren’t the only factors that influence privacy levels.Cultural, moral, and metaphysical

[152]See Bennett, C.J. and Raab, C.D., The Governance of Privacy. Policy Instruments in Global Perspective, M.I.T. Press, Cambridge, Massachusetts 2006, 2nd ed., chapt. 1.

[153]See, e.g., Schwartz, P.M., The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, American Journal of Comparative Law 1989, vol. 37, p. 675–701; Ruiz, B.R., Privacy in Telecommunications: A European and an American Approach, Kluwer Law International, The Hague / London / Boston 1997; Eberle, E.J., Dignity and Liberty: Constitutional Visions in Germany and the United States, Praeger, Westport, Connecticut 2002, p. 88–94.

[154]See, e.g., the U.K. Data Protection Act of 1998 and Denmark’s Personal Data Act of 2000 (Lovnr. 429 af 31. maj 2000 om behandlingafpersonoplysninger).

[155]see, e.g., Lunde, A.S., Huebner, J., Lettenstrom, G.S., Lundeborg, S., Thygesen, L., The Person-Number Systems of Sweden, Norway, Denmark and Israel, U.S. Department of Health and Human Services; Vital and Health Statistics : Series 2 ; no. 84; D.H.H.S. Publication No. (P.H.S.) 80-1358, Washington, D.C. 1980.

influences all play a role. Attitudes toward the importance of private life, attitudes toward the worth of people as individuals, and attention to noneconomic and emotional needs of people are all important. In cultures that espouse political values, such as those of Mill, Locke, Constant, and Madison, privacy is a major concern. As Lukes points out, privacy is "probably the fundamental concept of liberalism" in the context of a "sphere of thinking and action that should be free from 'public' intervention."[156]

The liberal love for privacy is evident in the establishment of privacy-protection legal frameworks. Western democracies have the most comprehensive regimes. In most African and Asian countries, on the other hand, such regimes remain underdeveloped. It's tempting to see this situation as symptomatic of African and Asian cultures' proclivity for prioritizing the group's desires and loyalties at the detriment of the citizen. However, it is important to avoid categorizing countries and cultures into rigid groups.

2.6 LET'S SUM UP

The differences between the different data security regimes are also highlighted in this chapter. As a result, it is appropriate to conclude with a few short observations on the prospects for greater global harmonisation of regulatory regimes. To put it bluntly, comprehensive economic harmonisation is incredibly difficult to happen anytime soon. This is due in part to the global strength of entrenched ideological/cultural disparities.As previously stated, such divisions exist even within representatives of the Western, multicultural, democratic sphere, and they will not go away easily. Future foreign policymaking in the region will have to negotiate seriously with nations and communities outside of the sphere, which will make bridging gaps much more difficult. Another consideration is the absence of a solid, dynamic, and representative international body capable of bridging the gap.

2.7FURTHER READING

- Reidenberg, J.R., Resolving Conflicting International Data Privacy Rules in Cyberspace, Stanford Law Review, 2000, vol. 52, p. 1315–1371.
- Rossnagel, A., Pfitzmann, A., Garstka, H., Modernisierung des Datenschutzrechts, report for the German Federal Ministry of the Interior (Bundesministerium des Innern), September 2001.
- Regan, P.M., Legislating Privacy: Technology, Social Values, and Public Policy, University of North Carolina Press, Chapel Hill / London 1995.

[156] See, e.g., Moore, B., Privacy: Studies in Social and Cultural History, M.E. Sharpe, New York 1984; Roberts, J.M. and Gregor, T., Privacy: A Cultural View, in Pennock, J.R. and Chapman, J.W. (eds.), Privacy: Nomos XIII, Atherton Press, New York 1971, p. 199–225; Altman, I., Privacy Regulation: Culturally Universal or Culturally Specific?, Journal of Social Issues 1977, vol. 33, p. 66–84.

- Hughes, G.L. and Jackson, M., Hughes on Data Protection in Australia, Law Book Co. Ltd., Sydney 2001, 2nd ed.
- Solove, D., Understanding Privacy, Harvard University Press, Cambridge, Massachusetts 2008, chapters 1–2.
- Inness, J.C., Privacy, Intimacy, and Isolation, Oxford University Press, New York / Oxford 1992, chapter 2.

2.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Which country has used boldest approaches while formulating data privacy laws?**

The French law expresses the broadest, if not the most audacious, set of goals: “Information technology should be at the disposal of any citizen.” It will be established in the sense of international collaboration. It does not infringe on people’s identities, rights, anonymity, or personal or public liberties.”

2.9 ACTIVITY

Elaborate the measures used for facilitating identification of persons (i.e., personal data) in order to safeguard the privacy and related interests of those persons.

3

Unit 3: EUROPEAN DATA PRIVACY LAW DEVELOPMENTS

Unit Structure

3.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- General data protection regulation
- Personal data processing principles
- Natural person's right to delist from search engine
- Privacy shield

3.2 INTRODUCTION

Some of the most significant European data privacy law developments that have emerged since the European Union adopted the Data Protection Directive in 1995 occurred in the year 2014. These include the adoption of the European Union's General Data Protection Regulation ("GDPR"), the invalidation by the Schrems decision of the U.S.–EU Safe Harbor cross-border data-transfer framework, and the subsequent replacement of the Safe Harbor framework with the EU-U.S. Privacy Shield. The "right to delisting," which the 2014 Google Spain decision created, also experienced continued development. This survey reviews the GDPR's main provisions—arguably the most important recent development - and then discusses the other developments noted above.[157]

3.3ADOPTION OF THE GENERAL DATA PROTECTION REGULATION

On April 27, 2016, the European Union finally adopted the GDPR, more than four years after the European Commission proposed it. The regulation came into force on May 24, 2016 and it will become applicable starting May 25, 2018 when it will repeal the current Data Protection Directive. This gives companies until May 2018 to adapt to its new provisions.[158]

European Union data protection law protects individuals (natural persons, as opposed to corporate entities or legal persons), which it refers to as "data subjects," with respect to their personal data processing. The GDPR defines both "processing" and "personal data" broadly and in adherence with the Data Protection Directive, even though it reorganizes and updates the Data Protection Directive's definitions.[159] Processing with respect to personal data may include, but is not limited to, the

[157] Voss, W.. (2017). European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. Business Lawyer, The. 72. 221.

[158] Dove, Edward. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law, Medicine & Ethics. 46. 1013-1030. 10.1177/1073110518822003.

[159] Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

following: “collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, era- sure or destruction.” The relevant personal data are” any information relating to an identified or identifiable natural person (‘data subject’),” and may include location data, online identifiers, and other forms of information that may be used to identify a data subject directly or indirectly, in addition to classic identifying data such as names and identification numbers.

The following sections address a few of the GDPR provisions that differ significantly from the Data Protection Directive and are important for businesses.

3.3.1TERRITORIAL SCOPE

The GDPR’s territorial scope is larger than that of the Data Protection Directive. The personal data processing place no longer controls the analysis; instead, under the GDPR, processing merely must occur “in the context of the activities of an establishment of a controller or a processor in the Union,” a definition that expands the analysis to include the activities of the processor that processes personal data on behalf of the data controller.[160] The GDPR also applies to the “pro- cessing of personal data of data subjects who are in the [European] Union by a controller or processor not established in the [European] Union” so long as the processing is related to “the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union” or the monitoring of such data subjects’ behavior “as far as their behaviour takes place within the [European] Union.” For example, the GDPR applies to a U.S. provider’s cloud-based-services offering to individuals in the European Union, even where the offering requires no payment and the provider has no establishment in the European Union, to the extent that the offering involves processing those individuals’ personal data.[161]

3.3.2PERSONAL DATA PROCESSING PRINCIPLES

Although the GDPR’s personal data processing principles are similar to those in the Data Protection Directive, there are a few differences. For example, the GDPR explicitly requires data to be processed “in a transparent manner,” but the Data Protection Directive only implicitly requires transparency.[162] In addition, the GDPR specifies that in accurate data must be erased or rectified “without delay,” adding a time element to the “accuracy” principle already contained in the Data Protection Directive.[163] Finally, the “accountability” principle requires the controller to be able to

[160] GDPR, supra note 3, art. 99(1), at 87 (“This regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.”). The date of its publication in the Official Journal of the European Union was May 4, 2016.

[161] GDPR, supra note 3, art. 4(1), at 33. Compare Directive 95/46, supra note 1, art. 2(a), at 38 (defining “personal data”).

[162] GDPR, supra note 3, art. 3(1), at 32. Compare Directive 95/46, supra note 1, art. 3, at 39 (addressing scope). The consideration of a processor’s activities in determining the territorial scope of the GDPR reflects the greater accountability of processors under the GDPR, when compared to the Data Protection Directive.

[163] GDPR, supra note 3, art. 5(1)(a), at 35 (“processed lawfully, fairly and in a transparent manner”). Compare Directive 95/46, supra note 1, art. 6(1)(a), at 40 (“processed fairly and lawfully”).

demonstrate compliance with the other personal data processing principles. This latter provision ties into the new GDPR record- keeping obligations discussed in Section II.G.

3.3.3LEGITIMATE PROCESSING BASES, INCLUDING CONSENT

The GDPR retains the requirement that a legitimate basis must exist in order for personal data processing to be lawful. It further develops the "purpose limitation" principle, allowing the controller to evaluate whether personal data processing for a purpose other than the one for which the data were originally collected enjoys such a basis, where it is not based on the law or the data subject's consent. This compatibility determination considers, among other things, links between the two purposes, context (including the relationship between the data subject and the controller), the data's nature (specifically, whether special data categories are involved), possible consequences for the data subject, and the existence of "appropriate safeguards," which could include data encryption orpseudonymization.[164]

Where consent is the processing basis, it must be unambiguous. The Data Protection Directive provided that "the data subject's consent" meant "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." The GDPR similarly defines data subject "consent" but provides the additional requirement that the data subject's wishes be "unambiguous" and manifested "by statement or by a clear affirmative action."

The GDPR sets out additional conditions for such consent beyond those contained in the Data Protection Directive, including a requirement that the controller be able to demonstrate that the data subject has given his or her consent. If a declaration that covers other matters contains a consent request, the request must be clearly written and distinguishable from those matters, with one risk for non-compliance being that the declaration's consent request will be non- binding. These requirements encourage good recordkeeping and proper document drafting.

3.3.4DATA-SUBJECT RIGHTS

The GDPR requires transparency in the provision of information to data subjects about their rights and the means of exercising them. This requirement applies regardless of whether data are collected directly from the data subject or indirectly from a third party. Under the GDPR, data subjects continue to benefit from rights they had under the Data Protection Directive, such as the right to access, the right to object to processing (which they may exercise at any time when the processing is for direct-marketing purposes), and from the transparency-and accuracy-principle requirements discussed above, as well as the related right to rectification "without

[164] Compare Directive 95/46, supra note 1, art. 7(f), at 40 ("[P]ersonal data may be processed only if . . . processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party . . . .") (emphasis added).

undue delay."[165] A data subject has the right not to be subject to a "decision based solely on automated processing including profiling, which produces legal effects concerning him or her or significantly affects him or her," subject to certain exceptions, such as where the data subject provides explicit consent or where automated processing is necessary for a contract between the controller and the data subject.

The GDPR creates several new rights for data subjects beyond those provided by the Data Protection Directive. First, it creates a "[r]ight to erasure ('right to be forgotten')." This right is often dependent on the data subject meeting the criteria set out in the relevant clause (e.g., it is subject to there being no overriding legitimate grounds for the processing, where the data subject exercises his or her right to object to it), and may become inapplicable where processing is necessary for exercising the right of freedom of expression and information, for certain reasons based on the public interest, or for establishing, exercising, or defending legal claims. Furthermore, "taking account of available technology and the cost of implementation," a controller that has made data public before being required to erase it shall take "reasonable steps . . . to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of such data.

Moreover, a right to restrict processing may apply, either for a period of time for purposes set out in Article 18 of the GDPR, or as an alternative to data era- sure. The GDPR also creates a right to data portability, which allows data subjects to request the controller to return their data in a commonly used, machine- readable format, and to request that the controller transmit such data to another controller if the processing was based on consent and was carried out by auto- mated means. The right does not apply to processing that was necessary for public interest or official authority tasks, and it must not "adversely affect the rights and freedoms of others."[166]

Finally, European Union or Member State law may restrict certain data subject rights when the restriction "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard, among other things, national security, defense, the fight against crime, and the furtherance of justice.

3.4THE PRIVACY SHIELD

The European Commission/DoC negotiations led to the establishment of the "EU–U.S. Privacy Shield" and the corresponding European Commission draft adequacy decision. Attached to the draft adequacy decision are seven annexes from U.S. government entities that set out various commitments and requirements, such as increased data subject protections and greater requirements for data controllers to respect data protection principles, including purpose limitations.[167] One improvement from a data subject perspective is greater opportunity for recourse through an independent recourse mechanism provided by the data controller. In addition, under

[165] Compare Directive 95/46, supra note 3, art. 12, at 42

[166] GDPR, supra note 3, art. 17(1)(c), at 44.

[167] Mark Scott, In Europe-U.S. Clash on Privacy, a Longstanding Schism, N.Y. TIMES (Oct. 7, 2015), http://nyti.ms/1Q93iJM.

this new frame work, an individual data subject may invoke binding arbitration of claims pursuant to the Privacy Shield principles under certain conditions. Furthermore, the Federal Trade Commission ("FTC") will review non-compliance allegations "to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated," potentially resulting in enforcement action under the FTC Act. Moreover, the DoC has committed to providing greater oversight and Privacy Shield compliance monitoring.[168]

Following data protection authority comments, the parties modified the EU-U.S. Privacy Shield to include "additional clarifications on bulk collection of data, strengthening the Ombudsperson mechanism, and more explicit obligations on companies as regards limits on retention and onward transfers,"[169] and they adopted the final implementing decision with revised annexes. The Privacy Shield became operational on August 1, 2016.

3.5GOOGLE AND THE RIGHT TO DELISTING

In the 2014, Google Spain case, the court granted a natural person the right to compel delisting of newspaper pages containing information prejudicial to him when Internet users searched for his name using a search engine. Google sought to limit the right's geographic scope to European web domains, while the French data protection authority ("CNIL") sought to have the delisting extended to all relevant domains including ".com."[170] The CNIL issued an order to that effect, which Google contested, prompting the CNIL to commence a formal procedure against it.

On March 10, 2016, the CNIL Restricted Committee imposed a €100,000 fine on Google. In doing so, it rejected Google's offer that it would "filter results based on the geographic origin of the person performing the search," meaning that "people using the search engine from the same country [as] the plaintiff's country [could] not access the delisted result anymore." The CNIL commented that "[o]nly delisting on all of the search engine's extensions, regardless of the extension used or the geographic origin of the person performing the search, can effectively uphold" the right to privacy. Google announced that it was appealing the decision to the highest French administrative court.

3.6 LET'S SUM UP

The European Union has finally adopted data protection law reform, and now is the time for companies to adapt to the new landscape before the GDPR applies in May

[168] See European Commission Unveils EU-U.S. Privacy Shield, EUR. COMM'N (Feb. 29, 2016), http:// ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm.

[169] Commission Implementing Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, C (2016) 4176 final (July 12, 2016) [hereinafter Draft Commission Implementing Decision], http://ec. europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

[170] See Commission Implementing Decision of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EUU.S. Privacy Shield, C (2016) 4176 final (July 12, 2016) and Annexes 1 to 7, http://ec.europa.eu/ justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf and http://ec.europa.eu/ justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf.

2018. Many of the GDPR's provisions address companies' compliance obligations and require greater accountability and recordkeeping. Some provisions may require changes to internal organization (e.g., DPOs, DPIAs, and procedures that allow for proper data breach notifications). The United Kingdom's DPA issued a checklist of steps to prepare for the GDPR. These include raising awareness, documenting held personal data, reviewing privacy notices to bring them into conformity with the GDPR, checking that procedures cover all data subject rights and adapting them to cover handling data subject requests, identifying legal bases for processing, implementing systems to verify ages of children and to gather parental or guardian consent, implementing procedures regarding data breaches, designating DPOs if required, and identifying any applicable supervisory authorities.

With respect to cross-border personal data transfers, companies may now self-certify under the Privacy Shield. They should monitor developments regarding the right to delisting, as this affects access to information on the Internet.

In conclusion, it is clear that EU data protection and privacy law reform over the past year will necessarily require adaptation by companies and others for years to come.

3.7FURTHER READING

- Press Release, Eur. Comm'n, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016).
- CouncilDirective95/46,1995O.J.(L281)31(EC)[hereinafterDirective95/46].
- Case C-131/12, Google Spain SL v. AgenciaEspan˜ ola de Proteccio´n de Datos (AEPD), 2014E.C.R. 317,

3.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Why did the need for adoption of The General Data Protection Regulation arise?**

   European Union data protection law protects individuals (natural persons, as opposed to corporate entities or legal persons), which it refers to as "data subjects," with respect to their personal data processing.

3.9 ACTIVITY

Elucidate the principles adhered to while adopting The General Data Protection Regulation. (1000-1500 words)

4

Unit 4: REGULATORY POLICY ON DATA PROTECTION

4.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- International Instruments on Data Protection
- Impact of Data Protection regulatory regimes
- National Data Protection regimes in Europe

4.2 INTRODUCTION

This section provides an overview of the main legal instruments at both international and national levels which deal directly with data protection. Some account is also taken of instruments which formally are not legally binding but are, nevertheless, highly influential in development of regulatory policy in the field. Many, if not most, countries' legal regimes contain a multitude of laws that reflect aspects of the fundamental principles usually found in data security instruments or that may otherwise facilitate the realization of these principles, but in haphazard, ad hoc ways. Data protection, breach of trust, slander, and intellectual property laws are only a few examples. The following review is largely concerned with the extent to which countries have implemented rule-sets that are explicitly dealing with fostering data security.The extent to which countries allow for the creation of autonomous bodies (hereinafter referred to as "data protection authorities") expressly tasked with monitoring the enforcement and/or further advancement of these rule-sets is also of primary concern.[171]

4.3INTERNATIONAL INSTRUMENTS

The formal normative basis for data protection laws derives mainly from catalogues of fundamental human rights set out in certain multilateral instruments, notably the Universal Declaration of Human Rights (U.D.H.R.), the International Covenant on Civil and Political Rights (I.C.C.P.R.) along with the main regional human rights treaties, such as the European Convention on Human Rights and Fundamental Freedoms (E.C.H.R.) and the American Convention on Human Rights (A.C.H.R.). All of these instruments – with the exception of the African Charter on Human and People's Rights – expressly recognise privacy as a fundamental human right. The omission of privacy in the African Charter is not repeated in all human rights catalogues from outside the Western, liberal-democratic sphere. Individuals have a right to privacy, according to the Cairo Declaration on Human Rights in Islam (see Article 18(b) – (c)). Other civil rights, such as freedom from oppression and freedom of speech, are also applicable in these instruments, while the right to privacy is closely tied to the values and concepts of data protection legislation.[172] The fact that

[171] MeitY, Feedback on Draft Personal Data Protection Bill, available at https://meity.gov.in/content/feedback-draft-personal-data-protection-bill.

[172] Park, Sungmi&Akatyev, Nikolay & Jang, Yunsik& Hwang, Jisoo& Kim, Donghyun& Yu, Woonseon& Shin, Hyunwoo& Han, Changhee& Kim, Jonghyun. (2018). A comparative study on data protection legislations and

data protection policies often point out protection of that right as fundamental to their formal logic reflects the particular value of the right to privacy in this sense. It is also reflected in case law developed pursuant to I.C.C.P.R. Article 17 and E.C.H.R. Article 8: both provisions have been authoritatively construed as requiring national implementation of the basic principles of data protection laws with respect to both the public and private sectors.[173]

In reality, these laws serve as data security instruments in and of themselves. However, case law is yet to enforce them in terms that greatly expand on the standards already present in other data security laws, and the defense they actually provide falls short of that provided by many of the latter instruments in several cases. There is no genuinely universal agreement or protocol dealing directly with data security in all international legal instruments. Calls for such an instrument are increasingly made, and work is underway to draft an appropriate set of international rules on point. Yet while there is clearly a need for a global legal approach in the field, there is, realistically, scant chance of, say, a U.N.-sponsored convention being adopted in the short term. The closest to such an instrument at present is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "C.o.E. Convention"). Although this is a European instrument, it is envisaged to be potentially more than an agreement between European states as it is open to ratification by states not belonging to the Council of Europe, though only upon the Council's invitation (see Article 23).[174] Civil society representatives have recently pushed to get non-member states to take advantage of this possibility though it is too early to tell whether this initiative will bear fruit. At present, the Convention has yet to be ratified by a non-member state. As for the E.U., its constitutional instruments now recognise that protection of personal data is in itself (i.e., separate from the broader right to privacy) a basic human right. This is a significant and hitherto unique development at the international level.

The main international conventions concerned directly with data security seek to encourage not only the enactment but also the harmonisation of national laws. The harmonisation goal has many justifications, some of which are less concerned with data security and more concerned with promoting the exchange of personal data across national boundaries in order to sustain international trade, freedom of speech, and intergovernmental cooperation.The latter worries arise because many national data protection laws, mostly in Europe, have long imposed restrictions on data flow to countries that do not provide comparable levels of data protection to the "exporting" jurisdiction. Although the functional influence of such rules on actual transborder data flow has been minimal, their potential impact has caused considerable concern, particularly among business interests. The A.P.E.C. Guidelines, the O.E.C.D. Guidelines, and the O.E.C.D. Guidelines all express concern about minimizing this effect in order to protect trade.[175]

government standards to implement Digital Forensic Readiness as mandatory requirement. Digital Investigation. 24. S93-S100. 10.1016/j.diin.2018.01.012.

[173] Bennett, C. J. (2011). Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies. *Journal of Comparative Policy Analysis,13*(2), 125–141.

[174] Credit China. (2018). *E-Commerce Integrity Convention*. *Credit China Shandong Qingdao Website*, 12 June 2018

[175] Custers, B., et al. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law and Security Review,34*(2), 234–243.

Privacy Framework and E.U. Directive. The latter goes the furthest in securing regional transborder data flow by prohibiting E.U. member states from instituting privacy-related restrictions on data transfer to other member states (see Article 1(2)). This ban stems from the need to expedite the completion of the EU's internal economy. Around the same time, however, the Directive goes the furthest of the foreign instruments in limiting transborder data exchange, by its competent restriction of data transmission to non-E.U. states that refuse to have "adequate" standards of data security (Article 25).

Despite their harmonising objectives, the international instruments tend to leave countries a significant degree of leeway in development of their respective data protection regimes. This is particularly true of "soft law" instruments. The legally binding instruments, on the other hand, provide for a great deal of national versatility. The C.o.E. Convention isn't meant to be self-executing, and it allows for major exceptions.Although the E.U. Directive has more prescriptive "bite" than its predecessors, it is only intended to facilitate "approximation" rather than total uniformity of national rules (see particularly recital 9 in its preamble). As a result, it gives EU member states a lot of space to maneuver.

About forty countries have passed data security legislation, and the number is increasingly increasing. The majority of these nations are European. Indeed, at both the national and regional levels, Europe has the oldest, most detailed, and bureaucratically burdensome data security regulations. Furthermore, as previously said, Europe serves as a springboard for the most aggressive and comprehensive foreign projects in the region, owing to its supranational institutions.[176]

The following are common points of departure for national data security regimes in Europe:

- coverage in both the public and private sectors;
- coverage in both automated and manual systems for processing personal data, largely regardless of how the data was structured;
- application of broad definitions of "personal data;"
- application of extensive sets of procedural principles, some of which are seldom seen in other data protection regimes;
- more stringent regulation of such types of personal data
- restrictions on transborder flow of personal data;
- establishment of independent data protection agencies with broad discretionary powers to oversee implementation and creation of data protection rules;
- channeling of privacy complaints to these agencies instead of courts;
- extensive subjection of data processing to notification and/or licensing requirements administered by the data protection agencies.

[176] Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law and Security Review,34*(3), 477–495.

- little use of industry-developed codes of practice.[177]

While the bulk of these characteristics are typical for national data protection regimes in Europe, each country there has its own unique mix of rules; concomitantly, a good deal of variation exists in the degree to which each country shares the above-listed traits. For example, the Netherlands has already used industry-based codes of conduct to a large extent, and the E.U. Directive promotes wider use of such codes (see Article 27). Furthermore, each country's data security regimes are far from uniform.

For example, Swedish law initially worked with reasonably stringent licensing and notice provisions; now it has dispensed completely with a licensing system, cut down drastically on notification requirements and implemented "light-touch", misuse-oriented regulation for the production of unstructured electronic data. There has been movement too at a broader European level. For instance, while many early European data protection regimes relied heavily on paternalistic control mechanisms (i.e., control exercised by government bodies (primarily data protection agencies) on behalf and supposedly in the best interests of citizens (data subjects)), they now show greater readiness to rely more on participatory control (i.e., control exercised by citizens themselves), supplemented by greater readiness to embrace market mechanisms for regulation of data processing. This notwithstanding, European jurisdictions (in contrast to, say, the U.S.A.) generally still maintain a relatively non-negotiable legislative baseline for the private sector.[178]

Across the Atlantic, Canada and Argentina come closest to embracing the European approach. Canada has federal legislation in place aimed at ensuring comprehensive protection of personal data in relation to both the public and private sectors. All Canadian Provinces and Territories have also enacted data protection legislation in relation to provincial and territorial government agencies; the legislation of several provinces also covers the private sector. Data protection agencies exist at both federal and provincial levels. The E.U. Commission (hereinafter "European Commission") has formally ruled that, in general, Canada offers "adequate" protection for personal data pursuant to Article 25 of the E.U. Directive. As for Argentina, it enacted legislation in 2000 modelled on the E.U. Directive and equivalent Spanish legislation, and formally based on the right of habeas data provided in its Constitution (Article 43). Like with Canada, the European Commission has formally ruled that Argentina satisfies the E.U. Directive's adequacy criterion.[179] Mexico might well be joining this "adequacy" club in the not too distant future as it has fairly comprehensive data protection legislation in place for the public sector and similar legislation for the private sector was recently passed by the Mexican Senate. It has also established a data protection authority (Federal Institute of Access to Information and Data Protection).

By contrast, European-style data protection authorities do not exist in the U.S.A. and its legal regime for data protection is relatively atomised. While there is quite

[177] European Commission. (2018). *The GDPR: new opportunities, new obligations*. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf.

[178] Gao, H. (2018). EU personal data protection practices and enlightenment. *Secrecy Science and Technology,9*, 53–59

[179] Goncalves, M. E. (2020). The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research,23*(2), 139–152.

extensive legislation dealing with federal government agencies, omnibus legislative solutions are eschewed with respect to the private sector. Legal protection of data protection in relation to the latter takes the form of ad hoc, narrowly circumscribed, sector-specific legislation, combined with recourse to litigation based on the tort of invasion of privacy and/or breach of trade practices legislation. At the same time, though, a “safe harbour” agreement has been concluded between the U.S.A. and E.U. allowing for the flow of personal data from the E.U. to U.S.-based companies that voluntarily agree to abide by a set of “fair information” principles based loosely on the E.U. Directive. Despite slow corporate take-up in its early days, the scheme now has over 2000 corporations (including major businesses) formally certifying adherence to it. Although the European Commission has determined that the scheme satisfies the Directive’s adequacy test in Article 25, considerable evidence has since accrued to indicate significant shortcomings in the scheme’s effectiveness in delivering real privacy protection.

In the Asia-Pacific region, there exist a handful of relatively comprehensive legislative regimes on data protection – most notably those in Australia, New Zealand, Hong Kong, South Korea and Japan. The bulk of these jurisdictions – but not Japan – have also established data protection authorities. New Zealand has been the fastest and most ambitious of these jurisdictions in the data protection field; it was the first to enact data protection legislation applying across the public and private sectors. Australian, South Korean and Japanese legislation in the field was initially limited largely to regulating the dataprocessing activities of government agencies, but has since been extended to cover the private sector as well.However, some of these expansions do leave significant coverage holes in the private sector. Some elements of the legislation in question deviate from the European Union paradigm as well (s). The European Commission is yet to officially recognize any of the countries involved as providing appropriate security under the EU Directive.

Data protection regimes in other Asia-Pacific jurisdictions tend to be even more patchy in coverage. Malaysia, for instance, has recently introduced data protection legislation to cover parts of the private sector but lacks equivalent legislation for personal information processed by government agencies.[180]Singapore has so far decided to establish a data protection regime based largely on voluntary, self-regulatory schemes that are linked with its national trust mark programme. As for the People’s Republic of China, there exists formal constitutional protection for privacy-related interests, augmented by a patchwork of sectoral laws on point. There have been signals over recent years that the country is on the verge of introducing relatively comprehensive data protection legislation, but no such law has yet been enacted. Much the same can be said of India. Although the country has previously been reported to be considering enactment of a data protection law modelled on the E.U. Directive (largely due to fear that its burgeoning outsourcing industry will flounder without such legislation in place),no such law has yet emerged. Legal regimes for data protection are least developed in Middle Eastern and African countries taken as a whole.

As noted above, the African Charter on Human and People’s Rights of 1981 omits mentioning a right to privacy in its catalogue of basic human rights. Moreover, the bulk of African countries have yet to enact European-style data protection laws. Nonetheless, some such laws have recently emerged, chiefly in francophone African

[180]Helsper, E. J., &Reisdorf, B. C. (2017). The emergence of a “digital underclass” in Great Britain and Sweden: Changing reasons for digital exclusion. *New Media and Society,19*(8), 1253–1270.

states, such as Burkina Faso, Tunisia, Morocco and Mauritius. This development partly reflects efforts by the French data protection authority (Commission de l'Informatique et des Libertés (CNIL)) to cultivate data protection in former French colonies, but it also reflects economic concerns, particularly the desire by some of these countries to safeguard their outsourcing industry (the case with, e.g., Tunisia and Morocco). Of the non-francophone states, the Republic of South Africa has come furthest along the path to establishing a comprehensive legal regime on data protection. Section 14 of its Bill of Rights, found in Chapter 2 of its 1996 Constitution, makes explicit provision for a right to privacy. A general right to access to records maintained in both the public and private sectors is also included (in section 32). In 2002, law focused on the above right was passed, and progress is currently underway on a bill for separate data privacy legislation.

As for the Middle East, Israel has long had a legislative regime for privacy and data protection in place and has been recently assessed by the E.U.'s Article 29 Working Party as passing the E.U. adequacy test. And, as noted above, Dubai passed data protection legislation in 2007 – the first (and hitherto only) Arab state to do so. That legislation, however, applies only to the Dubai International Financial Centre, not to data-processing activities in the rest of Dubai.

4.4RELATIVE IMPACT OF REGULATORY REGIMES

Comparative analysis of the effects of the different regulatory systems discussed above is both difficult and fraught with pitfalls. The task's complexity stems in part from the many facets of impact measurement: impact must be assessed in terms of economy (i.e., the cost of setting up the regime), efficiency (i.e., the cost of the regime compared to its practical results), effectiveness (i.e., the extent to which the regime's practical results achieve its ultimate goals), and equity (i.e., the extent to which the regime's practical results achieve its ultimate goals) (i.e., the extent to which the regime extends protection equitably across social groups).[181]The fact that each country's data security regime consists of more than just formal legislative regulations further complicates matters. Although the latter, along with structured oversight processes, are essential components of a data protection policy, they are augmented by a complex number of other instruments and structures – such as database systems, business codes, and guidelines – that affect the operational effect of the legal rules at the same time. The functioning of a data protection regime (including, of course, the extent to which "law in books" equates with "law in practice")[182] will also be shaped by a myriad of relatively informal customs and attitudes which prevail in the country concerned – e.g., the degree to which the country's administrative and corporate cultures are imbued with reverence for authority or values of "equal knowledge." Many of these variables, it goes without saying, are quickly misunderstood or misinterpreted. Because of their nature, it cannot be concluded that a data protection body with strong institutional powers would often be more effective in achieving its goals than one with less formal powers.Another complicating factor is that certain data protection authorities'

[181]Qin, S. (2018). *Research on the protection of personal information in the context of e-commerce in China*. Hebei: Hebei Normal University.

[182]Ren, Y., Cheng, F., Peng, Z., Huang, X., & Song, W. (2011). A privacy policy conflict detection method for multi-owner privacy data protection. *Electronic Commerce Research,11*(1), 103–121.

enforcement approaches may obscure their constructive accomplishments. Rather than openly reaching out with threats of economic penalties, agencies frequently tend to settle controversy in a comparatively discreet manner requiring “backroom” negotiation. Furthermore, authorities are often almost as concerned, if not more so, with preventing an unrealized opportunity for privacy-invading activity as they are with offering a solution after such activity happens. Measuring the effect of anticipatory control is more complex than measuring the impact of reactive, ex post facto control.[183]

Finally, some fair criticisms of data security regimes in general should be considered. One line of critique is that the regimes have yet to cultivate an institutional emphasis, as shown by the lack of direct regulatory support for privacy-enhancing technology. Another point of contention is the judiciary’s marginalization; in many nations, courts have played little, if any, active role in creating and implementing data privacy regulations.This condition not only results in a lack of definitive advice on how to view the applicable laws correctly, but it also leads to data protection’s marginalization as a legal area.

4.5 LET’S SUM UP

As for harmonisation efforts at the regional level, the track record of A.P.E.C. is yet to be firmly established. Within the E.U. – home to the hitherto most ambitious efforts – harmonisation remains incomplete. A large question mark hangs also over the ability of the E.U. to bring the data protection regimes of non-European states in line with its preferred model. This is presently due not so much to the recent emergence of A.P.E.C. as a potential competitor in the role of data protection “superpower”; there is as yet little evidence to show that A.P.E.C. can offer close competition in this regard. Rather, the weak implementation of Articles 25–26 in the E.U. Directive is more immediately critical. How those rules are implemented, constitutes an important litmus test for the Directive’s international credibility and success. Significant problems with E.U. member states’ implementation of those rules are noted above. The European Commission’s tardiness in issuing adequacy findings exacerbates these problems. In the space of over a decade, only a handful of countries have so far received an adequacy stamp – and most of them are scarcely major powers in a global context.This tardiness is not surprising: proper adequacy assessments are inevitably intricate, time-consuming tasks. Unfortunately for the Directive, its regime for transborder data flow to third countries is caught between “a rock and a hard place”: if properly implemented, the regime is likely to collapse from the weight of its cumbersome, bureaucratic procedures. Alternatively, it could well collapse because of large-scale avoidance of its proper implementation due precisely to fears of such procedures.

4.6FURTHER READING

- Wunsch-Vincent, S., WTO, E-Commerce, and Information Technologies: From the Uruguay Round through the Doha Development Agenda, Report for U.N. I.C.T. Task Force (Markle Foundation 2005).

[183] Ryz, L., &Grest, L. (2016). A new era in data protection. *Computer Fraud and Security,2016*(3), 18–20.

- Bygrave, Where have all the judges gone? Reflections on judicial involvement in developing data protection law, in Wahlgren, P. (ed.), IT ochjuristutbildning. Nordisk årsbokirättsinformatik 2000, Jure AB, Stockholm 2001, p. 113– 125;
- European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, Brussels, 15th May 2003,.

4.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the common points of departure for national data protection regimes in Europe?**

   The common points of departure include coverage of both public and private sectors; coverage of both automated and manual systems for processing personal data largely irrespective of how the data are structured; application of broad definitions of “personal data and many more.

4.8 ACTIVITY

Elucidate the national data protection regimes in Europe. (1000-1500 words)

BAOU
Education
for All

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

○

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in