RGPVNOTES.IN

Program : **B.E**

Subject Name: **Cyber Law and Ethics**

Subject Code: **CS-8004**

Semester: **8th**

Human rights in cyberspace

Human rights in cyberspace is a relatively new and uncharted area of law. The United Nations Human Rights Council (UNHRC) has stated that the freedoms of expression and information under Article 19(**2**) of the International Covenant on Civil and Political Rights (ICCPR) include the freedom to receive and communicate information, ideas and opinions through the Internet.[1]

An important clause is Article 19(**3**) of the ICCPR, which provides that:

The exercise of the right provided in paragraph two of this article carries with it special duties and responsibilities. It may therefore be subjected to certain restrictions, but these shall only be such as are provided by law and are necessary:

(**a**) For respect of the rights or reputations of others;

(**b**) For the protection of national security or of public order, or of public health and morals.[1]

The HRC has stated that "the same rights that people have offline must also be protected online" (mentioning, in particular, freedom of expression).[2] It is widely regarded that this freedom of information must be balanced with other rights. The question is raised whether people's expectations of human rights are different in cyberspace.

FREEDOM OF SPEECH AND EXPRESSION IN CYBERSPACE

In Union of India v. Assn. for Democratic Reforms the Supreme court said :“One sided information, disinformation, misinformation and non-information, all equally create an uninformed citizenry which makes democracy a farce. Freedom of speech and expression includes right to impart and receive information which includes freedom to hold opinions”.

U/A 19 of our constitution reasonable restrictions can be imposed on this fundamental right on several grounds.

Some people advocate there should be complete freedom on speech and expression at least in cyberspace. Some extended the geographical limits of this complete freedom to the physical world by doing events like AIB. They argue they deserve complete freedom everywhere and why only cyberspace.

Question is why we needed reasonable restrictions on this freedom till now?

Article 19(2) of the Indian constitution enables the legislature to impose certain restrictions on free speech for issues –

I. security of the State,
II. friendly relations with foreign States,
III. public order,
IV. decency and morality,
V. contempt of court,
VI. defamation,
VII. incitement to an offence, and
VIII. sovereignty and integrity of India.

Reasonable restrictions on these grounds can be imposed only by a duly enacted law and not by executive action.

But if we analyse recent trends or content on internet , we see despite obvious violations we are willing to accept offensive public space expressions but not restrictions on them.

As the age old social dynamics of our human co-existence in social structures are evolving to gain complexity and new dimensions due to so many fundamental life changes enabled by technological advancements, need for better and more flexible and accommodating laws is increasing.

Some ask why do we need any regulation at all on this freedom to express. It is so fundamental to human lives that there should be no restriction on it at all.

Do we need any restriction or not?
How much is acceptable to the healthy ever-rising consciousness in democratic setup?

Even if the concept of nation-state is slowly melting and we all live in a global village. Society need a structure for coordination and cooperation based on universal human values for advancement of humanity on a sustainable path.

Need for social structure implies we need well defined individual spaces for peaceful and beneficial co-existence of all in this web of social life. Now individual spaces need not be concrete compartments but will have to be flexible plastic walls.

What should be the elasticity of this plastic wall material is the question ? It should be flexible enough to accommodate decent criticism, disagreements etc. but it should be plastic enough to ensure a dignified secure individual space.

The underlying philosophy of this needed architecture of social existence will have to be in sync with the ever evolving dynamic cultural context.

Such a requirement of modern existence demand we retain the simplicity but add innovative design thinking in law making. This is a challenging and resource intensive task.

Are we prepared for that refinement in our approach to law making and its implementation?

Now, What should be the structure for cyberspace content growth/evolution?

Cyberspace has emerged as an integral part of reality we live in. How do we plan to use this space/arena? Should it have a structure of itself for a systemic evolution of this space reality or should it be allowed to grow in wilderness without artificial structural needs ?
For this we need to decide on which one is better from existential perspective?

At best i can think of an analogy – In real life we have natural factors and artificial structures operating simultaneously to co-create this beautiful reality we have been living in for ages. In my personal opinion in cyberspace too we need a mix of wilderness of free expression and some structural laws to co-create a meaningful cyber reality contributing to existential reality co-evolution in best possible manner.

I don't deny that it is perfectly possible to think of and come up with some other ingenious system design that is better but for that we need to first be sure of whats the boundary of reality we have been living in. Only then we will be able to create a better system than this. I think we are still far far away from being fully clear about the reality we are living in. It will take us time to understand it fully, till then in my opinion we can safely assume the above mentioned analogy example to be a decently good guiding strategy.

Right to Internet access

The **right to Internet access**, also known as the **right to broadband** or **freedom to connect**, is the view that all people must be able to access the Internet in order to exercise and enjoy their rights to freedom of expression and opinion and other fundamental human rights, that states have a responsibility to ensure that Internet access is broadly available, and that states may not unreasonably restrict an individual's access to the Internet.

Ensuring that access is broadly available and preventing unreasonable restrictions[edit]

Several countries have adopted laws that require the state to work to ensure that Internet access is broadly available or preventing the state from unreasonably restricting an individual's access to information and the Internet:

- Costa Rica: A 30 July 2010 ruling by the Supreme Court of Costa Rica stated: "Without fear of equivocation, it can be said that these technologies [information technology and communication] have impacted the way humans communicate, facilitating the connection between people and institutions worldwide and eliminating barriers of space and time. At this time, access to these technologies becomes a basic tool to facilitate the exercise of fundamental rights and democratic participation (e-democracy) and citizen control, education, freedom of thought and expression, access to information and public services online, the right to communicate with government electronically and administrative transparency, among others. This includes the fundamental right of access to these technologies, in particular, the right of access to the Internet or World Wide Web."[13]
- Estonia: In 2000, the parliament launched a massive program to expand access to the countryside. The Internet, the government argues, is essential for life in the 21st century.[14]
- Finland: By July 2010, every person in Finland was to have access to a one-megabit per second broadband connection, according to the Ministry of Transport and Communications, and by 2015, access to a 100 Mbit/s connection.[15]
- France: In June 2009, the Constitutional Council, France's highest court, declared access to the Internet to be a basic human right in a strongly-worded decision that struck down portions of the HADOPI law, a law that would have tracked abusers and without judicial review automatically cut off network access to those who continued to download illicit material after two warnings[16]

- Greece: Article 5A of the Constitution of Greece states that all persons have a right to participate in the Information Society and that the state has an obligation to facilitate the production, exchange, diffusion, and access to electronically transmitted information.[17]
- Spain: Starting in 2011, Telefónica, the former state monopoly that holds the country's "universal service" contract, has to guarantee to offer "reasonably" priced broadband of at least one megabit per second throughout Spain.

Right to privacy

What is privacy?

Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.

Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information.

The rules that protect privacy give us the ability to assert our rights in the face of significant power imbalances.

As a result, privacy is an essential way we seek to protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us, while protecting us from others who may wish to exert control.

Privacy is essential to who we are as human beings, and we make decisions about it every single day. It gives us a space to be ourselves without judgement, allows us to think freely without discrimination, and is an important element of giving us control over who knows what about us.

Why does it matter?

In modern society, the deliberation around privacy is a debate about modern freedoms.

As we consider how we establish and protect the boundaries around the individual, and the ability of the individual to have a say in what happens to him or her, we are equally trying to decide:

- the ethics of modern life;
- the rules governing the conduct of commerce; and,
- the restraints we place upon the power of the state.
  Technology has always been intertwined with this right. For instance, our capabilities to protect privacy are greater today than ever before, yet the capabilities that now exist for surveillance are without precedent.

  We can now uniquely identify individuals amidst mass data sets and streams, and equally make decisions about people based on broad swathes of data. It is now possible for companies and governments to monitor every conversation we conduct, each commercial transaction we undertake, and every location we visit. These capabilities may lead to negative effects on individuals, groups and even society as it chills action, excludes, and discriminates. They also affect how we think about the relationships between the individual, markets, society, and the state. If the situation arises where institutions we rely upon can come to know us to such a degree so as to be able to peer into our histories, observe all our actions, and predict our future actions, even greater power imbalances will emerge where individual autonomy in the face of companies, groups, and governments will effectively disappear and any deemed aberrant behaviour identified, excluded, and even quashed.

  Perhaps the most significant challenge to privacy is that the right can be compromised without the individual being aware. With other rights, you are aware of the interference -- being detained, censored, or restrained. With other rights, you are also aware of the transgressor -- the detaining official, the censor, or the police.

  Increasingly, we aren't being informed about the monitoring we are placed under, and aren't equipped with the capabilities or given the opportunity to question these activities.

  Secret surveillance, done sparingly in the past because of its invasiveness, lack of accountability, and particular risk to democratic life, is quickly becoming the default.

  Privacy International envisions a world in which privacy is protected, respected and fulfilled. Increasingly institutions are subjecting people to surveillance, and excluding us from being involved in decisions about how our lives are interfered with, our information processed, our bodies scrutinised, our possessions searched. We believe that in order for individuals to participate in the modern world, developments in laws and technologies must strengthen and not undermine the ability to freely enjoy this right.

Is privacy a right?

Privacy is a qualified, fundamental human right. The right to privacy is articulated in all of the major international and regional human rights instruments, including:

United Nations Declaration of Human Rights (UDHR) 1948, Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." International Covenant on Civil and Political Rights (ICCPR) 1966, Article 17: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

An important element of the right to privacy is the right to protection of personal data. While the right to data protection can be inferred from the general right to privacy, some international and regional instruments also stipulate a more specific right to protection of personal data, including:

- the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,
- the Council of Europe Convention 108 for the Protection of Individuals with Regard to the Automatic Processing of Personal Data,
- a number of European Union Directives and its pending Regulation, and the European Union Charter of Fundamental Rights,
- the Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2004, and
- the Economic Community of West African States has a Supplementary Act on data protection from 2010.
  Over 100 countries now have some form of privacy and data protection law.

However, it is all too common that surveillance is implemented without regard to these protections. That's one of the reasons why Privacy International is around -- to make sure that the powerful institutions such as governments and corporations don't abuse laws and loopholes to invade your privacy.

Right to data protection

What is data protection?

Personal data is any information relating to you, whether it relates to your private, professional, or public life. In the online environment, where vast amounts of personal data are shared and transferred around the globeinstantaneously, it is increasingly difficult for people to maintain control of their personal information. This is where data protection comes in.

Data protection refers to the practices, safeguards, and binding rules put in place to protect your personal information and ensure that you remain in control of it. In short, you should be able to decide whether or not you want to share some information, who has access to it, for how long, for what reason, and be able to modify some of this information, and more.

Governments also have a security interest in ensuring the protection of personal data. In 2015, criminals stole 21.5 million records from the US Office of Personnel Management that contained the highly sensitive personal data of federal employees and their family members. This type of attack is happening more frequently across the globe, and countries must take action to better protect individuals' information.

Why do we need data protection laws?

There are two main reasons that governments should pursue comprehensive data protection frameworks:

- **Laws need to be updated to address today's reality**. Ever since the internet was created, people have been sharing more and more of their personal information online. In many countries, privacy rules exist and remain important to help protect people's information and human rights, but they are not adapted to suit the challenges of today's connected world.
- **Corporate co- and self-regulation is not working to protect our data**. Around the world, companies and other entities that collect people's data have long advocated for regulation of privacy and data protection not through binding frameworks but rather through self- or co-regulation mechanisms that offer them greater flexibility. However, despite several attempts, we have yet to see examples of non-binding regimes that are positive for users' rights

The Right to Data Protection

Privacy and data protection are two rights enshrined in the EU Treaties and in the EU Charter of Fundamental Rights.

The Charter contains an explicit right to the protection of personal data (Article 8).
The entry into force of the Lisbon Treaty in 2009, gave the Charter of Fundamental Rights the same legal value as the constitutional treaties of the EU. Thus the EU institutions and bodies and the Member States are bound by it.

In addition, article 16 of the Treaty on the Functioning of the European Union (TFEU) obliges the EU to lay down data protection rules for the processing of personal data. The EU is unique in providing for such an obligation in its constitution.

Data Protection Law

For decades, the EU has held high standards of data protection law . The law entitles individuals to exercise specific data protection rights and obliges (public or private sector) organisations that process their data to respect these rights.

In April 2016, the EU adopted a new legal framework - the General Data Protection Regulation (GDPR) and the Data Protection Directive for the law enforcement and police area.

Fully applicable across the EU in May 2018, the GDPR is the most comprehensive and progressive piece of data protection legislation in the world, updated to deal with the implications of the digital age.

It applies to organisations or companies not established in the EU who offer goods and services to individuals in the EU or monitor their behaviour. It creates new rights for individuals in the digital environment and several new and detailed obligations for cooperation.

Globally, there is an increasing growth in data protection (sometimes referred to as data privacy in non-EU countries) laws. Many of these laws are strongly influenced by the EU rules, which have long been considered the gold standard in data protection law.

Over 100 countries around the world now have data protection laws in place: fewer than half of these countries are in Europe (28 EU Member States and others). The majority of data protection laws have been adopted outside of Europe, with the fastest growth seen in African countries.

Cyber crime and legal frameworks

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information,

business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cybercrime may also be referred to as computer crime.

Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyberterrorism are also of significant concern.

Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:

- Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks.
- Crimes that use computer networks to advance other criminal activities. These types of crimes include cyberstalking, phishing and fraud or identity theft.

The FBI identifies cybercrime fugitives who have allegedly committed bank fraud and trafficked counterfeit devices that access personal electronic information. The FBI also provides information on how to report cybercrimes, as well as useful intelligence information about the latest cybercriminals

Types of Cybercrime

DDoS Attacks

These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

Botnets

Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

Identity Theft

This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.

Cyberstalking

This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

Social Engineering

Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information. Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.

PUPs

PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download.

Phishing

This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many

of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.

Prohibited/Illegal Content

This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

Online Scams

These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are “too good to be true” and when clicked on can cause malware to interfere and compromise information.

Exploit Kits

Exploit kits need a vulnerability (bug in the code of a software) in order to gain control of a user’s computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

legal frameworks - ??

Categories of Cyber Crime

Cyber Crimes against Individuals, Institution and State

Cyber crimes are broadly categorized into three categories, namely crime against

1. Individual
2. Property
3. Government

Each category can use a variety of methods and the methods used vary from one criminal to another.

Individual: This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

email spoofing

Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation.Although most spoofed emails can be easily detected and require little action other than deletion, the more malicious varieties can cause serious problems and pose security risks. For example, a spoofed email may pretend to be from a well-known shopping website, asking the recipient to provide sensitive data such as a password or credit card number. Alternatively, a spoofed email may include a link that installs malware on the recipient's device if clicked

Cyberstalking

This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

Spamming

Spamming is the use of electronic messaging systems like e-mails and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately. The term spamming is also applied to other media like in internet forums, instant messaging, and mobile text messaging, social networking spam, junk fax transmissions, television advertising and sharing network spam.

Hacking

Hacking generally refers to unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.Hacking can also refer to non-malicious activities, usually involving unusual or improvised alterations to equipment or processes.

institutions

As a regulated sector, financial institutions, including banks, are greatly affected in the event of cyber-attacks, such as a data breaches. These institutions have to pay fines and penalties for losing personal identifiable information. They also tend to lose the most business and customers after a cyber-attack.

In India, there have been quite a few instances of banks losing valuable information to cyber criminals, through different kinds of cyber-attacks.

The following are a few of the vulnerabilities of financial institutions.

Account takeovers: Cyber criminals have demonstrated their ability to exploit the internet of things, especially the online interface between financial and market systems, such as automated clearing house (ACH) systems, card payments, and market trades.

Payment systems: Fraudulent monetary transfers and counterfeiting of stored value cards are one of the most common cyber-attacks against financial institutions, payment processors, and merchants.

ATM skimming: ATM skimming is a common cyber-crime in India, similar to other countries. In this crime, a criminal installs a skimming device on an ATM to collect card numbers and personal identification number (PIN) codes. Point of sale terminals: Point of sale (POS) terminals in India are a prime target for cyber criminals in India. Credit and debit cards from many financial institutions were affected by cyber-attack events that target POS terminals.

Mobile banking exploitation: As more mobile devices are being introduced in personal, business, or government networks, they are many instances of PIN thefts. Cyber criminals have successfully used man-in-the-middle attacks against mobile phones using malwares. It is a technique where the attacker secretly relays and alters the communication between two parties who believe they are communicating with each other

Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government

websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

- **Rioting and Inciting Riots**
- Learn about where the line is drawn between protest and rioting, how inciting riots is defined under the law, the federal penalties for a conviction, and more.
- **Sedition**
- An overview of the federal crime of sedition, in which two or more people conspire to overthrow the government or oppose the legal authority of the U.S. by force.
- **Terrorism and Terroristic Threats**
- The basics of terrorism, terroristic threats, and how United States law punishes such actions, including an explanation of what constitutes terrorism, related offenses, and sentencing.

- **Espionage**
- Explanation of the federal crime of espionage, which prohibits the sharing of classified government documents and other sensitive information with unauthorized individuals or organizations.
- **Treason**
- How the United States Codes defines the serious crime of treason, in which a U.S. citizen or legal resident has levied war against the country or given aid to its enemies.
- **Flag Burning**
- A summary of flag burning as an act of protest, which is protected under the First Amendment to the U.S. Constitution, but which was once treated as a serious crime.

Hacking

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

Who is a Hacker? Types of Hackers

A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

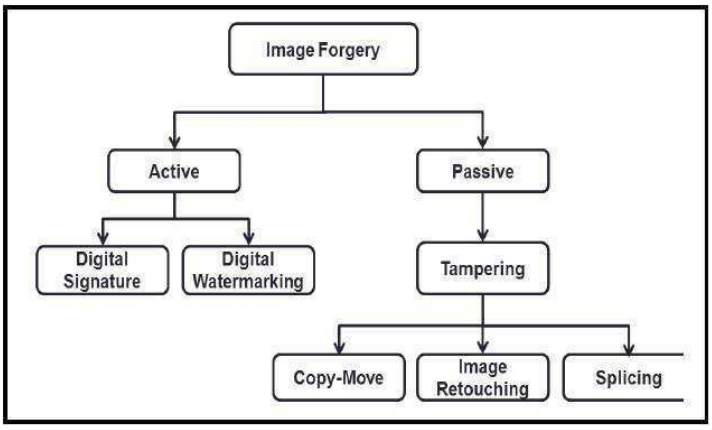
Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Description
Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetrationTesting and vulnerability assessments.
Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
Script kiddies: A non-skilled person who gains access to computer systems using already made tools.
Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

Digital forgery

Forgery has been defined as the crime of falsely altering or manipulating a document with the intension of misleading others. It may include the production of falsified documents or counterfeited items. Today, we live in the digital era, where digital technology has become predominant technology for creating, processing, transmitting, and storing information [1]. Digital forgery is falsely altering digital contents such as pictures, images, documents, and music perhaps for economic gain. It may involve electronic forgery and identity theft. The majority of digital forgery occurs because digitally altered pictures often appeal to the viewers' eyes. And with the availability of powerful, affordable picture-processing software (such as Adobe Photoshop, Adobe Premiere, Corel Draw, or GIMP), one can alter almost anything in a photo. For example, images of children (child pornography) involved in sexually explicit conduct can be created from innocent images, or even without the involvement of an actual child [2]. Digital techniques are notoriously more precise than conventional means of retouching because any area of the photo can be changed pixel by pixel. It is hard for humans to spot images that have been doctored in some way. Thus the common saying “seeing is believing” is no longer true in this digital age

The digital image has become one of the most important means of sending and receiving information. It is the foremost source of evidence for any event in the court of law. It is also used in forensics investigations, military, medical records, insurance, and other fields. There are three types of image forgery: image retouching, splicing forgery, copy-move image forgery. They are illustrated in Figure 1 [3]. Regardless of the camera used to take pictures, image retouching can be used to get rid of any flaws later on. Retouching manipulates the image by changing its features without making noticeable modifications of the content. Splicing (i.e. copy paste) is a form of photographic tampering in which there is digital splicing of two or more images into a single composite. Perhaps the most common type of forgeries is the copy-move (i.e. cloning) forgery. In this forgery type, a part of the image itself is copied and pasted into another part of the same image with the aim of concealing certain features in the original images [4].



4. FORGERY DETECTION

As digital cameras replace analog ones, the need for authenticating digital images and detecting forgeries increases. Recent advances in technology have provided methods for detecting unethical uses of digital forgery. These include techniques for detecting cloning, splicing, resampling artifacts, color filter-array aberrations, and chromatic aberrations [5

Forgery detection techniques can be classified into two broad categories [6]: active and passive or blind. Typical examples of active technique are watermarking and steganography . Copy move forgery detection is a common example of passive technique. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are popular algorithms for effective transformation of an image. They are both used for copy-move forgery detection [7]. Lighting inconsistencies in digital images can be used for revealing traces of digital tampering. Artificial blurring is another common process in digital image manipulation; it is used to generate plausible digital image forensics.

Cyberstalking

What is Cyberstalking?

Cyberstalking is a relatively new concept, and there has yet to be a universally agreed-upon definition. However, most organizations that specialize in this area have definitions that contain the same elements:

- Stalking is done with the assistance of technology (typically the internet) rather than in person
- It is done to make a person feel afraid, threatened, or worried about their safety

- It invades a person's privacy
- The stalker monitors the victim's behavior, threatens them, or makes unwanted advances
- The behavior is unwanted

While stalking can be done by a stranger, most victims know their stalker. Motives for stalking range, but typically include seeking attachment, revenge, or reconciliation from the victim.

Cyberstalkers engage in numerous behaviors, all aimed at making their victims feel embarrassed, harassed, threatened, or afraid. Some of the most popular tactics include:

- Catfishing, or pretending to be someone else online to get close to a victim – often with the goal of obtaining private information or photos
- Doxing, or the act of publishing private information online
- Monitoring their victim's whereabouts using social media check-ins and location tags
- Hijacking their victim's webcam
- Viewing metadata on images or other files, including geotags
- Sending unwanted messages
- Hacking online accounts
- Online identity theft
- Flaming, or slandering the person online

Cyberstalking Legislation

In the United States, cyberstalking is a criminal offence. Slander, harassment, and anti-stalking legislation laws govern cyberstalking to some degree. In addition, it is covered in the Violence Against Women Act and other federal acts. Unfortunately, these pieces of legislation do not adequately address all instances of cyberstalking, leaving it to state legislators to enact protective laws. California lead the way in 1999 with the first anti-cyberstalking law passed at the state level. Since then, 13 other states have followed suit:

- Using an electronic device, computer, or email communication to harass a person is prohibited under laws enacted by New York, New Hampsire, Illinois, Hawaii, Connecticut, Arizona, and Alabama

- Messages sent electronically are covered by anti-stalking laws in California, Wyoming, Oklahoma, Florida, and Alaska, with Florida strengthening this legislation to include an outright ban on cyberstalking in 2003
- Stalking through electronic means is banned in Texas
- Stalking and harassment using electronic means as well as cyberbullying are banned in Missouri

In jurisdictions without specific cyberstalking laws, the act itself may still be prohibited through anti-harassment legislation.

How to Protect Yourself

Cyberstalking can happen to anyone at any time. Since most victims already know their stalker, it is never too early to review your online behavior to mitigate your risks and keep yourself protected.

- Review your privacy settings on all accounts, including social media and email
- Turn off geotagging and location sharing on all devices
- Never use a location tag feature, like Facebook's "check in" option, when uploading photos
- Set strong passwords and never use the same password twice
- Google yourself to see how much information is available, and take steps to limit anything private
- Use a VPN whenever you are browsing online, especially when using public Wi-Fi networks

Cyber pornography

Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.

Cyber pornography is banned in many countries and legalized in some. In India, under the Information Technology Act, 2000, this is a grey area of the law, where it is not prohibited but not legalized either.

Under Section 67 of the Information Technology Act, 2000 makes the following acts punishable with imprisonment upto 3 years and fine upto 5 lakhs:

1. Publication- which would include uploading on a website, whats app group or any other digital portal where third parties can have access to such content.
2. Transmission- this includes sending obscene photos or images to any person via email, messaging, whats app or any other form of digital media.
3. Causing to be published or transmitted- this is a very wide terminology which would end up making the intermediary portal liable, using which the offender has published or transmitted such obscene content. The Intermediary Guidelines under the Information Technology Act put an onus on the Intermediary/Service Provider to exercise due diligence to ensure their portal is not being misused.

Section 67A of the Information Technology Act makes publication, transmission and causing to be transmitted and published in electronic form any material containing sexually explicit act or conduct , punishable with imprisonment upto 5 years and fine upto 10 lakhs.An understanding of these provisions makes the following conclusions about the law of cyber pornography in India extremely clear:

1. Viewing Cyber pornography is legal in India. Merely downloading and viewing such content does not amount to an offence.
2. Publication of pornographic content online is illegal.
3. Storing Cyber pornographic content is not an offence.
4. Transmitting cyber pornography via instant messaging, emails or any other mode of digital transmission is an offence.

However, there is one case in which viewing Cyber pornography is punishable with imprisonment upto 5 years and fine upto 10 lakhs. Where the content contains children engaging with one another or with adults in sexually explicit acts.Browsing or downloading Child pornography online is also a punishable offence under the Information Technology Act. The creation of child pornography is also punishable under the Act.The act of collecting and storing

cyber pornography is not an offence, but if the content involves minors, then it is punishable with imprisonment upto 5 years and fine upto 10 lakhs.

Identity Theft & Fraud Cyber terrorism

What is Identity Theft

Identity theft is the crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity to make transactions or purchases. Identity theft is committed in many different ways. Some identity thieves sift through trash bins looking for bank account and credit card statements; other more high-tech methods involve accessing corporate databases to steal lists of customer information. Once they have the information they are looking for, identity thieves can ruin a person's credit rating and the standing of other personal information.

Types of Identity Theft

Types of identity theft include criminal, medical, financial and child identity theft. In criminal identity theft, a criminal misrepresents himself as another person during arrest to try to avoid a summons, prevent the discovery of a warrant issued in his real name or avoid an arrest or conviction record.
In medical identity theft, someone identifies himself as another person to obtain free medical care. In financial identity theft, someone uses another person's identity or information to obtain credit, goods, services or benefits. This is the most common form of identity theft.

In child identity theft, someone uses a child's identity for various forms of personal gain. This is common, as children typically do not have information associated with them that could pose obstacles for the perpetrator, who may use the child's name and Social Security number to obtain a residence, find employment, obtain loans or avoid arrest on outstanding warrants. Often, the victim is a family member, child of a friend or someone else close to the perpetrator.

High-Tech Identity Theft

Identity thieves increasingly use computer technology to obtain other people's personal information for identity fraud. To find such information, they may search the hard drives of stolen or discarded computers; hack into computers or computer networks; access computer-based public records; use information gathering malware to infect computers; browse social networking sites; or use deceptive emails or text messages.

Identify Theft Protection

Many types of identity theft can be prevented. One way is to continually check the accuracy of personal documents and promptly deal with any discrepancies. Lots of businesses provide products that help people avoid and mitigate the effects of identity theft. Typically, such services provide information helping people to safeguard their personal information; monitor public records, as well as private records such as credit reports, to alert their clients of certain transactions and status changes; and provide assistance to victims to help them resolve problems associated with identity theft. In addition, some government agencies and nonprofit organizations provide similar assistance, typically with websites that have information and tools to help people avoid, remedy and report incidents of identity theft.

4. What is Cyber Terrorism?

There is often a large amount of confusion as to what cyber terrorism is. More specifically, what cyber attacks can we actually define as acts of terrorism? The internet has allowed for a vast exchange of information. Thus has created a cyber space in which both criminals and terrorists can implement attacks/communications. This use of cyber space results in there no longer being simply a physical threat of terrorism. When we consider what cyber terrorism actually is, we must first understand the motivations behind cyber attacks. Cyber attacks can come in many differing forms, and it is these forms that help us understand whether the attack is of crime or terror. Figure 1 shows the distribution of cyberattacks across cultural, social, economic and political motivations. Gandhi et al. (2011) discusses that often these dimensions of motivations can often cross over and the motivating factors behind cyber attacks are needed to be carefully considered when we discuss cyber terrorism.

4.3 Areas of Cyber Terrorism

As discussed many acts of cyber terrorism are often synonymous with acts of cyber crime. Thus the means by which attacks are implemented by terrorists may also be done by criminals. These can come in many forms, as discussed by GCHQ and Cert-UK (2015), attacks are often either un-targeted or targeted. These can include, though not limited to:

Un-targeted Attacks

• Phishing—These attacks typically involve fraudulent emails to convince a target of it's legitimacy of a user or organisation in order to attain private information (E.g, passwords, banking information, identity theft etc.) ("What are phishing scams and how can I avoid them?", 2017)

• Watering Hole—The deployment of a fake webpage to compromise the original, in order to attack visiting users (e.g the downloading of Remote Access Tools) (National Cyber Security Centre, n.d.)
• Ransomware—Infecting a system by encrypting files and/or locking the users access to said system. Then requiring a 'ransom' to gain normal access again. ("Protecting your organisation from ransomware", 2016)
• Scanning—Testing for vulnerabilities in specific internet networks or systems to deploy attacks on a wider scale to attack at random (GCHQ, Cert-UK, 2015).

Targeted Attacks
• Spear-Phishing—These attacks are much the same as the' Phishing' mentioned previously, however specifically targeted at an individual or organisation.
• Distributed Denial of Service—This is to deploy a mass amount of packet requests, often from a Botnet , to a 1 website or network in order to overload the system and prevent regular access by legitimate users.
• Supply chain—attacking an element of an organisation before it arrives (GCHQ, Cert-UK, 2015).
• Zero-day—Bespoke exploitation of a system with specific vulnerabilities not yet known to the author (National Cyber Security Centre, 2016).

Cyber Defamation

Cyber defamation in India

With the invention of the internet the life of a common has changed a lot. The internet has provided a medium to interact with the people worldwide. It has brought the world closer to every man who has access to it. It has proved to be repository of the enormous information which a common man could not access easily. It has also given new dimensions to business and trade. Social networking, entertainment, shopping, job hunt, recruitment, you name anything and its possible via the medium of internet.
The widespread use of internet has also given a new face to the crime and a new medium to the bad elements to commit crime.
Cyberspace is a technical term used for the electronic medium of computer networks, in which online communication takes place. It comes alive only when two or more computers are networked together. The term has a very wide meaning and is not only restricted to the internet but also includes computers, computer networks, the internet, data, software etc. The crimes that are committed by using the computer as an instrument, or a target or a mean for perpetuating further crimes falls within the definition of cyber crime. Cyber law

is the law that governs the crimes committed within the cyberspace. Cyber Defamation is also a cyber crime.

CYBER DEFAMATION

The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person. The injury can be done by words oral or written, or by signs or by visible representations. The intention of the person making the defamatory statement must be to lower the reputation of the person against whom the statement has been made in the eyes of the general public. Cyber defamation is a new concept but the traditional definition of the term defamation is application to the cyber defamation as it involves defamation of a person through a new and a virtual medium.

Cyber defamation is publishing of defamatory material against another person with the help of computers or internet. If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation. The harm caused to a person by publishing a defamatory statement about him on a website is widespread and irreparable as the information is available to the entire world. Cyber defamation affects the welfare of the community as a whole and not merely of the individual victim. It also has its impact on the economy of a country depending upon the information published and the victim against whom the information has been published.

The following are mediums by which offense of cyber defamation can be committed:

- World Wide Web
- Discussion groups
- Intranets
- Mailing lists and bulletin boards
- E-mail

There are two broad category of case falling under cyber defamation:

- The first category involves the cases in which the liability is of the primary publishers of the defamatory material, e.g. web site content providers, e-mail authors etc;
- The second category involves the cases involving the liability of the internet service providers or bulletin board operators.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in