University Institute of Legal Studies
Himachal Pradesh University

NAAC Accredited 'A' Grade University

SOUVENIR

National Seminar

On

Cyber Law and Cyber Crimes: Issues and Challenges

28th September, 2019

HIMACHAL PRADESH UNIVERSITY
(NAAC Accredited 'A' Grade University)
SUMMERHILL, SHIMLA -171005

Prof. (Dr.) Sikander Kumar
Hon'ble Vice- Chancellor

Message

These days computer and internet have become very common and necessary for the daily life. The increasing use of information technology facilitate the common people to get information, store information, share information etc. Today e-mail and websites have become the preferred means of date communication. As the use of internet is increasing, a new face of crime is spreading rapidly from in person crime to nameless and faceless crimes involving computers. Cyber Crime includes all unauthorised access of information and break security like privacy, passwords etc. With the use of internet Cyber Crimes also includes criminal activities performed by use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, cyber phishing, unauthorised access to computer system etc. There are various issues for identifying and proving cyber crimes. At present criminals have changed their methods and have started using advanced technology. All these issues needs to be addressed and public at the grass root level, as a awareness may prove a boon to tackle with cyber crimes.

I extend my best wishes to the organisers for conducting national seminar on this issue and I hope that it will provide a plate form for finding some solutions to this cyber Challenges.

Prof. (Dr.) Sikander Kumar

Ghanshyam Chand
Registrar

HIMACHAL PRADESH UNIVERSITY
(NAAC Accredited 'A' Grade University)
SUMMERHILL, SHIMLA -171005

Message

It give me immense pleasure that Himachal Pradesh University Institute of Legal Studies, Ava-Lodge Campus, Chaura Maidan, Shimla is going to organize one day National Seminar on vibrant theme Cyber Law and Cyber Crimes: Issues and Challenges on 28th September, 2019 at H.P. University, Auditorium. The advancement of technology has made man dependent on internet for all his needs. However with the development of the internet and its related benefits, has also developed the concept of Cyber Crimes. In matters of Cyber Crimes, India is also not for behind the other countries, where the rate of incidence of Cyber Crime is also increasing day by day. I am sure that the academicians, professionals, researchers and students will deliberate upon the important issues in various thematic areas and endow with useful recommendations to meet the challenges ahead.

On this occasion, I offer a warm welcome to the delegates who are coming here to participate in this one day national seminar from different parts of the country. I also wish to convey the organizers are the very best for the success of this seminar.

Ghanshyam Chand

HIMACHAL PRADESH UNIVERSITY
(NAAC Accredited 'A' Grade University)
SUMMERHILL, SHIMLA -171005

Prof. (Dr.) Arvind Kumar Bhatt
Dean, Planning and
Teacher's Affairs

Message

It is a matter of immense pleasure to learn that the Himachal Pradesh University Institute of Legal Studies, Ava-Lodge Campus, Shimla is organising a National Seminar on the topic **"Cyber Laws and Cyber Crimes: Issues and Challenges" on 28th September, 2019** wherein number of legal luminaries from different fields are expected to participate in this academic deliberation and a souvenir is also being decided to brought out to commemorate the occasion.

With the telecommunications and technological advances made at the dawn of the new millennium, the perception of India revolutionized in the world. The current paradigm shift in the IT world is no less dramatic and promises to transform our lives. At the same time, it is imperative that the law evolve in order to encourage the development of technology and progress and yet protect society from ills of cyber crime and abuse.

I compliment HPUILS, Shimla for organising a National Seminar which will definitely bring out some useful ideas and pragmatic suggestions. I extend my warm greetings to the organisers and wish the seminar every success.

Prof. (Dr.) Arvind Kumar Bhatt

HIMACHAL PRADESH UNIVERSITY
(NAAC Accredited 'A' Grade University)
SUMMERHILL, SHIMLA -171005

Prof. (Dr.) Sunil Deshta
Dean and Chairman
Department of Laws

Message

I am glad to know that University Institute of Legal Studies is organizing a National Seminar on Cyber Law and Cyber Crimes: Issues and Challenges on 28th September 2019.

The seminar is being organized on a very important issue of cyber crime. Presently almost whole of the population of India is a potential cyber user and is facing cyber crimes on regular basis that mostly go unreported. The reason behind this improper implementation of cyber law can be its lack of awareness and execution and in order to improve the prevailing scenario it becomes absolutely necessary to take initiatives and provide a platform for better understanding of cyber issues. The seminar would really provide an excellent opportunity to the academician, scholars coming from different parts of the country to share their views regarding the different aspects of cyber crime.

I hope that the Seminar would prove fruitful in disseminating the relevant information on prevention of cyber crime.

I congratulate the organizers for having taken such an initiative and wish seminar a good success.

Prof. (Dr.) Sunil Deshta

HIMACHAL PRADESH UNIVERSITY
(NAAC Accredited 'A' Grade University)
SUMMERHILL, SHIMLA -171005

Prof. (Dr.) Aman Kumar Sharma
Chairman,
Department of Computer Sciences

Message

A seminar is a place where true meeting of minds happen. Researchers, who would have done a good deal of thinking about their idea, will come forward and share their thoughts with fellow researchers. The beauty of a Seminar such as **National Seminar on Cyber Law and Cyber Crimes: Issues and Challenges** is that it allows such exchanges which in turn will ignite more ideas and ways of improving the presented ideas. The biggest beneficiaries hence will be the attendees who truly participate. The theme of the seminar is relevant to day to day life of one and all. I thank and congratulate the organizing team of University Institute of Legal Studies for placing in efforts in enabling awarenessthrough a seminar on the issue. The youth of today prefers to be connected online always. The cyberspace facilitates in numerous ways such as email, e-banking, social networking, online shopping, providing access to information, online gaming and much more with a click of a button. With the advancement in technologies many positives exist but the need of the hour is to be aware about the issues and challenges in terms of pitfalls of cyberspace. With the blurred boundaries between domains, technologies getting merged and less compelling technologies practically disappearing, we need to be updated on how our world is evolving and changing. We can use the national seminar to sensitize ourselves and add value to our research and our communities. I hope the outcome of the seminar will have concrete suggestions for the usage of internet. Wish you all a great event and enjoy.

Prof. Aman Kumar Sharma
Keynote Speaker

Dr. Rajneesh Khajuria
Department of Law

University of Jammu
Jammu and Kashmir

Message

Internet is the crucial technology of information age. It is influencing our lives in diverse ways and is a potential medium for information dissemination and information exchange as it makes temporal and spatial barriers irrelevant. Though it is changing the paradigms of the communication, business, education and governance, one cannot disregard the fact that it is also becoming a haven for the criminals. The wide variety of information that can be transferred, the open and unregulated nature of internet and the irrelevance of geography makes internet a fertile ground for criminal activities. This calls for need to have a proficient cyber law regime.

Cyber law is a recent phenomenon and it refers to all the legal and regulatory aspects of the internet and the World Wide Web. In the Indian context, the Information Technology Act, 2000 as amended by the I.T. Act, 2008 was passed by the Parliament to provide for the cyber legal infrastructure as the existing legal regime was not proficient in dealing with it. Besides, endowing legal recognition to Electronic records and Electronic signatures, it effectively deals with cyber crimes too.

The present National Conference on **Cyber Law and Cyber Crimes: Issues and Challenges** will help to understand the varied aspects of cyber laws and the challenges of Cyber Crimes in contemporary scenario. I congratulate the organizers for endeavoring to deliberate upon this theme as it will help to create awareness about cyber laws and also framing policies for its better execution. I wish all the success to the organizers.

Dr. Rajneesh Khajuria

HIMACHAL PRADESH UNIVERSITY
(NAAC Accredited 'A' Grade University)
SUMMERHILL, SHIMLA -171005

Prof. (Dr.) Sanjay Sindhu
Director, UILS
Dr. Veena Kumari
Assistant Professor. UILS

Message

In the developed world, the present generation cannot imagine a life without computers. Computers get associated with the person before his birth when scanner detects the pregnancy and growth and remain associated for same time even after death till insurance issues are settled. Modern technology has opened new channel. The cyber space is not an ethereal vacuum but a super highway of transmission of knowledge and information across space. The entire universe has become really small because the super highway traffic moves at as fast a pace as light. While all this has facilitated trading and other business related transactions involving billions of dollors every month, it has also given an opportunity to the deviant personalities to misuse the technology, although that too may be greatly innovative. Nevertheless, such an innovations entails no appreciation in the civilized world, even as it has not prepared itself to face such situation. Crimes which are directly associated with electronic Communication devices are generally called Cyber Crimes. Although, Information technology Act, 2000, which was further, amended in the form of IT amendment Act, 2008 was passed to deal with the offences related to computers, but there legislations do not include the definition of Cyber Crime. There are few other areas which requires to be duly addressed by the legislation. It is the high time to discuss and resolve these issues. I extend by best wishes to the organising institution to take initiative in this direction by conducting a national seminar. I hope that it will create awareness amongst masses towards the Cyber Laws and some valuable suggestions will be given by the illumineries.

Dr. Veena Kumari
Convenor

Prof. (Dr.) Sanjay Sindhu
Convenor

ABOUT THE SEMINAR: *CONCEPTUAL NOTE*

We are living in a society, which is called "Technologically Civilized" society. Today every other person is recognized with the device or gazette, he carries, which is technologically advance, thus it can be said that "living without technology is living without air" in this technical world of today. Technology made us dependent on it and we cannot expect or imagine a life without using a word "Technology" in it. One of the major areas of technology is information technology. Every one of us is a part of this cyber world, directly or indirectly, since computers and internet are the integral part of our life. Now-a-days everyone who works on the computer must be familiar with the terms cyber space and cyber crimes. India which is the fourth highest number of internet users in the world, has witnessed a dramatic rise in the number of cyber crimes in the cyber space. The latest statistics shows that cyber crime is actually on rice .However it is true that in India, cyber crimes are not reported too much. Consequently, there is a false sense of complacency that cyber crimes are not eminent threat. In order to carry out the attacks, the terrorists had used the most advanced form of technology. Thus these new technologies have posed new challenges before Governments, Law enforcing agencies, and individuals to safeguard the national as well as individual interests of the persons. The present seminar aims to create awareness about cyber laws, issues, challenges of cyber crimes towards the society among the students, academicians, professionals and others.

OBJECTIVES OF THE SEMINAR

The objective of the seminar is to trace out the Development of Technology and to discuss or deliberations on the following current areas.

- Dimensions of Cyber Law
- National and International Development of Cyber Law and Cyber Crimes
- Cyber Security and Secure internet
- Legal Challenges in Cyber laws.
- Relationship between internet rights and internet security
- Relationship of Cyber Law with Intellectual Property Rights
- Crimes against Women under Cyber Law
- Emerging Challenges before Cyber law
- Freedom, Security and Growth in Cyberspace
- Digital Democracy and Digital Diplomacy

Sub Themes for the Seminar:

It is rightly said that no one can change the world in one day but everyone can do their part. This will be a small initiative from our side to make world a better place to live in. The seminar will be graced by eminent speakers' i.e. Legal luminaries, academicians, researchers, students, members of Governmental and Non-Governmental Organization (NGOs) etc. engaged on the issues relating to the following themes in particular and sub-themes:

- Emerging Trends in Cyber World and law
- Role of UN for preserving Peace and Security in Cyber Space.

- Crime against Women in Cyber world(Cyber Obscenity and victimization)
- Crime against Children in Cyber world(Child Pornography, Sextortion, Indecent Representation)
- Crime against Government in Cyber world
- Privacy, Defamation & Data Protection in Cyber space
- Fake ID'S in Online Social Networks (OSNs) and Rule of Law
- Cyber Forensics & Electronic Evidence and Investigations
- Online-Consumers in Cyberspace
- Banking Financial Fraud, Scams and legal Protection in Cyber world
- Net Neutrality & Regulation of Internet in 21st century
- Artificial Intelligence and Cloud Computing & New Challenges
- Internet of Things, Block Chains – Emerging Challenges
- Data Security Concerns in cyberspace
- Crimes of Social Networking Sites (Social Media)
- Cyber Security Concerns in e- Commerce, Governance, e-Services, e- Banking
- Cyber Terrorism and Cyber Warfare
- Criminological Explanation of Cyber Crimes
- Regional Perspectives on the Cyber Space
- Cyber Security Laws and Policies in India and of other Countries
- Cyber Civility for Prevention of Cyber Bullying
- Cyber Sovereignty
- Cyber Voyeurism; An end of Privacy
- Military & Intelligence Actions in Cyber Space
- Lot & Operational technology Cyber Implications
- Cyber Extremism & Radicalization

CHIEF PATRON:

Prof. (Dr) Sikander Kumar
Hon'ble Vice Chancellor,
Himachal Pradesh University, Summer Hill, Shimla HP

PATRON:

Prof. (Dr)Sunil Deshta
Dean & Chairman, Department of Laws,
Himachal Pradesh University, Summer Hill, Shimla HP

CONVENOR(S)

Prof. (Dr) Sanjay Sindhu
Director, *UILS, Ava Lodge Campus,*
Himachal Pradesh University, Shimla HP

Dr. Veena Kumari
Assistant Professor, *UILS, Ava Lodge Campus*
Himachal Pradesh University, Shimla HP

ORGANISING SECRETARIES:

Dr.Kusum Chauhan , Assistant Professor, University Institute of Legal Studies
Dr. Gitanjali Thapar, Assistant Professor, University Institute of Legal Studies
Dr. Karuna Machhan, Assistant Professor, University Institute of Legal Studies
Ms. Ritika Rana, Assistant Professor, University Institute of Legal Studies

CONTACT DETAILS:

Prof. (Dr.) Sanjay Sindhu	94181-81797
Dr. Veena Kumari	94182-12464
Dr. Kusum Chauhan	94180-24222
Dr. Gitanjli Thapar	98166-71001
Dr. Karuna Machhan	94181-89262

National Seminar
On
Cyber Law and Cyber Crimes: Issues and Challenges

Index

Cyber Bullying and Law in India: A Critical Analysis

Dr. Lalit Dadwal, Associate Professor,
Department of Laws, H.P.University,Shimla ,
Email: lalitdadwal@gmail.com

Abstract

Cyber bullying is becoming a major concern surrounding the adolescent population because of the increased use in the internet and social networking sites. Studies show that cyber bullying can cause mental health concerns in adolescents who have been victimized, leaving them feeling lonely, depressed, and rejected. Cyber bullying is an emerging threat which is apparent through disgust speeches, harassment, cyber-stalking and forms of ridicule online and text messages. In an Ipsos survey in 2014, India topped the list of 254 countries for cyber bullying. 32% of parents surveyed in India said their children experienced cyber bullying, followed by Brazil (20%), Saudi Arabia (18%), Canada (18%) and the United States (15%). Parents in India also reported the greatest intensity of cyber bullying. 13% said a child in their home experiences cyber bullying on a regular basis, followed by 10% in Brazil, 5% in the United States and 5% in Argentina. As the main targets of cyber-bullying are children & teens, there is a threat of feeling unsafe, scared, being subjected to mental upset, defamation and the possibility of being driven to suicide. Legal issues relating to cyber bullying can be defamation on cyberspace, abetment of suicide, violation of privacy, cyber-stalking and obscenity. Cyber-bullying is a recent fact and there is very limited literature about the Indian stance on it. Cyber-bullying unlike other forms of bullying can happen 24X7 online through internet using computers and smart phones & there is no escape from it. This paper is an analysis of cyber-bullying in India in view of the exponential expansion of this problem in India and the rest of the world. The Information Technology Act and the Indian Penal Code are looked into to examine cyber-bullying. How liability should be imposed on minors committing cyber-bullying is also investigated. Researcher tried to analyze the problem from different perspective in order to try and find the possible solutions to reduce cyber bullying and educate the teenagers of its danger for both the victim and the perpetrator.

Keywords: Cyber-bullying, Information Technology Act, Online harassment, Social implications, Criminal Liability, Mens ria

Indian Digital Democracy: A Blessing Or Curse

Geeta, Research Scholar,
Punjab University, Chandigarh

Abstract

Indian democracy is world's democracy. From the 18th Century to the 19th Century continuance efforts were made for the development of Indian Democracy. Earlier, Indian democracy was described as representative democracy. But, with globalization, evolution of communication technology, the democracy shifted from representative to participatory democracy addressed as digital democracy making every voice audible. Digital democracy has been adopted with the agenda of public will, accountability and trust. As a result thereto, an opportunity provided to all the citizens to participate in the process of administration, decision making, policy making and service delivery by means of Chartrooms, Blogs, Interactive Survey and Face Book, Whatsapp, Twitter and other websites etc. Digital

democracy helped in curving corruption by minimizing gap between government and citizen and enhancing transparency and accountability of representatives in India. However, the democracy which was expected to provide more resilient to democracy has become more nemesis to democracy for the challenges, including phishing, fake or malicious news by "Bots" and Sock-popets, cyber attacks on databases, Face book, Whatsapp, Twitter, new apps embedded on smart phones and 'deep fake' videos Technology. Therefore, for making digital democracy, a blessing in India, some control on the means of information and communication technology are great need of present time.
Key Words: Indian Digital Democracy, information and communication technology, opportunities, challenges, transparency and accountability of representatives.

Cyber Law: A Knight In Shining Armor For The Digitally Driven World?

Darshan V, Vijay Sudarshan,
SASTRA Deemed to be University.

Abstract

Laws were made to regulate the human behavior and to maintain peace within a society. With various inventions and discoveries in the field of technology happening at a rapid pace there was a need for the law to even regulate the digital field and start to regulate it. Cyber law was mainly formulated to regulate and control the cyber attacks, cybercrimes and various other malicious activities which are nowadays done through the internet. The advent of internet came upon us like a blessing but as its wide capabilities were unveiled it started to look like more of a bane than of a boon. There are different classifications of cybercrime and they are against people, property and the government. To regulate the use of internet for the purpose of safety, security and privacy, the Information and Technology act was enacted in the year 2000.The goal of this study is to find out the various challenges faced by Cyber law and how these challenges are currently being tackled keeping the current technological resources. This paper also deals with the origin of the IT act and the various amendments made to it throughout the years. This study is about cyber law and the challenges faced by it and it also explore the various remedies available. It is anticipated that this paper will give a brief understanding to the people about Cyber law and the challenges faced by it in the digitally driven world of which we are increasingly becoming a part of.

A Brief Study On National And International Cyber Law

Sufiyan Firoz

Abstract

In the current world, technological advancements in information and communication technologies allow a large amount of data to be stored, accessed, searched, processed or transmitted, regardless of any geographical boundary. These advancements lead to new service that helps in economic development and dissemination of knowledge. However, with these developments, new crimes have also emerged and even the old one is being committed with new technologies. These crimes are kept under the head of Cyber Crime, which includes Spam, computer viruses, cyber attacks, identity attack etc. Cyber Crimes are the offences or crime that takes place over any electronic or informative system.

In 2003, malicious software has caused a damage of up to 17 billion USD. In 2007, damage by cyber crime reached 100 billion USD, which was more than the illegal drug trade. Moreover, 60 percent of businesses believe that cyber causes more harm than physical crime.

The above mentioned situation clearly shows that there is a dire need of reliable and effective cyber security. And enhancing the cyber security became a integral part national security and economic well being, governments are taking step and formulating laws to protect users.

This paper deals with the development that took place in the cyber world, cyber crimes and the law present to curb the offences. This paper also highlights the important cases that helped in shaping the cyber laws.

It is hoped that this paper will provide the audiences sufficient knowledge about the cyber crimes and cyber laws on both national as well as international sphere.

Keyword:- Cyber Crime, Data, information, communication

Cyber Crimes Vis-À-Vis Women

Poonam Langer, Student The Law School,
University of Jammu, Jammu & Kashmir, India

Abstract

The concept of Neo Criminology is an emerging one; dealing expressly with the advent of cyber crimes. It is pertinent to note that crimes against women are rampant especially in the cyber world. Cyber crimes have escalated manifold as they are easy to commit, difficult to detect and even harder to prove. The cyber crime victims are gravely affected by the aftermath of such crimes as even in the technological era of 21st century, the law lacks recognition of cyber crimes. Through this paper, I intend to deliberate upon the three major cybercrimes which are Cyber Stalking, Cyber Defamation and Cyber Pornography (including the modernistic buzz of revenge porn), their causes and the adverse ramifications. I shall also enumerate the laws in existence to shield women in these cases as u/s 67, 67A, 67B & 72 of the Information Technology (Amendment) Act, 2008 and the consequential advancement of laws as u/s 354, 354A, 354 B, 354 C & 354 D of the Criminal Amendment Bill (2013) in addition to IPC Provisions. The paper is supported by numerous leading cases such as the Ritu Kohli case, DPS MMS Scandal Case etc. At the outset, I would like to propose certain precautionary measures on part of women to desist the occurrence of cyber crimes against them. The paper also includes the recourse available to victims and the reforms necessitated in the legal system to effectively eliminate the expansion of cyber crimes that degrade the prestige and respectability of women in the society.

Cyber Law And Cyber Crimes: Issues And Challenges

Somya Vats And Suprita Surbhi,
Lloyd Law College, Greater Noida, Student

Abstract

The society we live in is not the one where ADAM and EVE lived, rather this is 21st century. Everything is fast in this era. Due to paucity of time, we choose to rely on artificial intelligence because of which digitalization has become one of the greatest achievement in the modern scenario which has resulted into being paperless arena. Just as a coin has two different sides in the same manner such improvisation has given wings to a number of cyber crime/offence. These are associated with the ill usage of computer. Crime such as stalking,

defamation, hate massages, unauthorized computer trespass and illegal possession of computerized information fall within the radar of cyber crime/offences. Even the government has also not left untouched from the malpractice of cyber crime which is popularly known as cyber terrorism. In order to have a control over these ill- practices several legislations has come into being. The Indian parliament has also taken cognizance over this matter and has incorporated two fold strategies to control the cyber crimes. It has amended Indian Penal Code to cover cyber crimes expressly and has provided provisions in the IT ACT, which were basically enacted to deal with computer related crimes India. Cyber crime is a growing phenomena and its complete reduction can only be attained when people keep themselves aware and cautious of the things which might take place with them while indulging into any online obligation.

Data Protection in India: Time to Add-on Writ of Habeas Data

Dr. Harish Verma,
Principal,
Jagran School of Law, Dehradun (Uttarakhand)
dr.harishthakur@gmail.com

Abstract

In age of digitalisation data security, privacy and data protection have become significant issues and posed numerous challenges to law makers. Individual's data in private and public domain are under severe threat to misuse owing to ineffective data protection laws and policy. Further, absence of individual's right to exercise control oversupplied personal data, has aggravated the problem. Cybercriminals use the internet and computer technology to hack user's personal details from social media. In many jurisdictions across the World, a Constitutional writ of *habeas data* is available to citizens to secure their privacy and personal information or data. This writ can be sought by any citizen against any manual or automated data register to find out what information is held about his or her person. That person can request the rectification and destruction of the data held. However, this *writ* has no specific legal recognition under Indian Constitution except that some of its facets are reflected in data protection laws. If like some other Constitutions of the World, *writ of habeas* data is included in Indian Constitution, it would be very useful in guaranteeing the protection against cyber-crimes and data misuse. Having this background in mind, the present study aims to examine data protection policies and laws in India to know the gaps in them. Also, the study intends to evaluate how the use of *writ of habeas data* can be more effective remedy for citizens to get their rights enforced from top courts of the country if it is made a part of Indian Constitution. The study is purely theoretical in nature based on secondary data taken from foreign laws, articles, journals and law books etc.

Key Words:-Habeas, Data, Writ, Privacy, Protection, Constitution, Remedy.

CRIME AGAINST WOMEN IN CYBER WORLD

Muskan & Muskan Singh, Student BA.LLB (Hon's) 3rd semester,
School of Law, Maharaja Agrasen university, Solan, HP

Abstract

Information technology has widened itself over the last two decades and has become the axis of today's global and technical development. The world of internet provides

every user all the required information fastest communication and sharing tool making it the most valuable source of information. With the numerous advancement of internet, the crime using internet has also widened its roots in all directions. The cyber-crimes pose a great threat to individuals. Cyber-crime is a global phenomenon and women are the soft targets of this new form of crime. In this paper we explore the Cyber-crimes and the online security vulnerabilities against women. Various issues that are discussed in this paper are: Cyber Stalking, Harassment via Email, Cyber Defamation, Morphing, and Email Spoofing against women, in a nutshell it talks about the cyber obscenity. Further it explores about the causes, objectives and its impact. It also briefly discusses about the numerous case laws and provision given under IT, Act 2000. It unfolds the Crime against women on internet is the one of the major issue which causes threat for the Indian women netizens are still not open to immediately report the cyber abuse or cyber-crime. This nature provides the offenders the chance to escape after the commission of cyber-crime. The problem would be solved only when the victimized woman then and there report back or even warn the abuser about taking strong actions. Cyber-crime is a national challenge

Analysing The Tax Challenges Due To Digitalisation Of The Economy: An Indian Perspective

Kanishka Sewak, Assistant Professor,,
School Of Law, Manipal University Jaipur

Abstract

The emergence cyberspace has created a borderless playing field for the Multinational Enterprises (MNE) where they shift the tax base from the country where the economic activity is done to the jurisdiction which has lower or zero corporate tax. The Organisation for Economic Co-operation and Development (OECD) along with G20 nations addressed the tax challenges arising due to digitalisation of the economy and prepared a report titled *Addressing the Tax Challenges of the Digital Economy.* This report was prepared under Action Plan 1, one of fifteen Action Plans that are part of Base Erosion and Profit Shifting (BEPS) package. As a follow-up measure, the Finance Ministers of G20 nations prepared an interim report in 2018 to concretise the plans of creating a Task Force on Digital Economy (TFDE) for observing the rise in tax avoidance and evasion due to digitalisation and suggest the ways to tackle this issue. These reports highlight the concern of significant rise in non-physical economic activities in countries including India making levy of taxes by authorities challenging. This paper is an attempt to study the proposals made by OECD and G20 for a country like India which is aggressively digitalising its economy without laying the groundwork for tax authorities to collect the fair share of taxes from MNEs that have significant business presence in one of the fastest growing economies that is India.

Keywords: Digital Economy, tax avoidance, BEPS, India

Cyber Stalking: Legal Position and Challenges in India

Dr. Kusum Chauhan ,Assistant Professor ,
University Institute of Legal Studies ,H.P. University, Ava-Lodge, Shimla,171004

Abstract

Exponential advances in the development and use of computer and other technologies have provided exciting, constructive opportunities for people’s advancement, productivity, and

enjoyment. However, these remarkable advances also have generated new arenas and tools for victimization. In a dynamic technological era, the whole world is in fingertips of the individual in second's time through the cyber medium popularly known as Internet. Besides having one of the largest numbers of Internet users in the world, India also has some of the highest statistics of sexual harassment globally. Harassment that women face 'offline' - on the streets, at home, or even at the workplace, is now being directed online as well. A crime only recently identified by government agencies and the news media is cyber stalking, or technology-aided stalking. Cyber stalking, or technology-aided stalking, is the use of electronic communications or tracking technologies to pursue another person repeatedly to the point of inducing fear. Cyber stalking can have major psychosocial impacts on individuals, such as increased suicidal ideation, fear, anger, depression, and post traumatic stress disorder symptomology.

Such crimes have not been given the kind of priority in India as these deserve. The mindset is such that these crimes are perceived as minor crimes. And going by the numbers, we know that by and large, India has failed in getting the requisite cyber crime convictions, and the number of such crimes is rising. When someone harasses you online, it is viewed by a much larger audience and you feel helpless about not being able to contain the spread of that false information or a photograph. So, the sense of shame, the trauma, the feeling of being exposed, is much, much higher. This paper explores the social, technical and legal perspectives of cyber stalking in India. Through this paper the researcher will try to review cyber stalking, its approaches, impacts, legal provision and measures to be taken to prevent it

Keywords: Cyber stalking, Internet, Law, Crime, Prosecute.

.Crime Against Women Under Cyber Law

Anjali Yadav And Mayank**,** Student**,** Ba Llb (4th Year) ,
Jims, School Of Law Affiliated To GGS IP University, G.Noida

Abstract

Though crime against women is on a rise in all fields being a victim of cybercrime could be most traumatic experience for a woman. In the digital age, Information and Communication Technology (ICT) is benefiting billions across the world by bridging certain gaps and multiplying human potential in every walk of life[1].

Technical measures to protect computer systems are being implemented along with legal measures to prevent and deter criminal behavior. But this technology knows no physical boundaries, it flows more easily around the world subsequently the criminals are increasingly located in places .Cybercrime against women in India is relatively a new concept. When India started her journey in the field of Information Technology, the priority was given to the protection of electronic commerce (e-commerce) and communications under Information Technology Act, 2000 whereas cyber socializing communications has remained untouched.

Dr.L.Prakash v. Superintendent[2] in this case the accused was an orthopedic surgeon forced women to perform sexual acts and later on upload and sale these videos as adult entertainment materials worldwide. He was charged under section 506 (part II of the section which prescribes punishment for criminal intimidation to cause death or grievous hurt), 367 (which deals with kidnapping or abduction for causing death or grievous hurt) and 120-B (criminal conspiracy) of the IPC and Section 67 of Information Technology Act, 2000 (which

dealt with obscene publication in the internet). He was sentenced for life imprisonment and a pecuniary fine of Rupees 1, 25,000 under the Immoral Trafficking (Prevention) Act, 1956.

The Act turned out to be a half baked law as the operating area of the law stretched Cyber Victimization of Women and Cyber Laws in India[3]. India is considered as one of the very few countries to enact IT Act 2000 to combat cybercrimes. This Act widely covers the commercial and economic crimes which is clear from the preamble of the IT Act.

An Analysis of The Emerging Trends Of Cyber Crime In India

Masoom Reza,Zeeshan Ahmad, Aman Prakesh Singh,
Student, Jamia Millia Islamia

Abstract

In this 21st century, the emergence of cyber space has reduced the whole world into a global village and the power of buttons has transcended the power of arms. The unprecedented information technology explosion in India, not only turned the country into a technology giant but also contributed to the outgrowth of unrestrained cyber crime. Fundamentally, the term Cyber crime is a generic expression for all acts/omissions which are done with criminal intent using the medium of computers and Internet and the involvement of virtual cyber medium at any stage of crime is sine qua non of such offences like Cyber-stalking, SMS/E-mail spoofing, Child pornography, Cyber squatting, Cyber vandalism and Cyber terrorism etc.

This paper attempts to delineate the various dimensions of the cyber crime which involves individuals, property, government and the society at large. In the light of the statistics and governmental/non-governmental reports, the basic reasons of such kind of offences, the problems faced by Children, women, corporate, and the government in the technologically advanced new India are holistically discussed.

Finally, after scrutinizing judicial pronouncements and legislative response of government to cyber crime, the major steps taken by the techno-giant nations are exhaustively analyzed. Moreover, various measures to deal with the emerging trends and rapid growth of cyber crime through Cyber incidence response mechanisms, with the collaboration of government and individuals , are recommended to achieve cyber security.

Liability Of Internet Service Providers Across Various Countries : An Overview

Poonam Pant And Bhumika Sharma,
LR Group of Institutions, Solan, H.P

Abstract

The role of ISP or Intermediary is very important for effective utilization of information technology. The liability of Intermediary or ISP has gain immense importance at international level. Various countries have defined the liability of ISP either in the form of copyright infringement or for the infringement of information technology. Australia was the first country to enact the legislation relating to the liability aspect of ISP in the form of Copyright Act, 1968 making ISP liable to disable the access to online services hosted outside Australia. Some safe harbours were also provided for ISP as part of the Australia - United States Free Trade Agreement. The US provides for the liability of ISP in the form of Communications Decency Act, 1996, Digital Millennium Copyright Act,1998. Title II of the DMCA

specifically deals with the issue of ISP liability and also provides for the penalties for unauthorized access to a copyright work. As regarding the legislations of Canada, it does not specifically define the liability of ISP, instead it provides safe harbor for those ISP's providing any means for Internet access. ISP's are also protected for copyright infringement in Canada. In Singapore the liability of ISP is regulated by the Internet class license and Internet code of Practice which requires the ISP to abide by the conditions of license. ISP's are also restricted to make public access of those websites which contain offensive content harmful to national interest. Japan's Copyright Act, 1970, The Provider Liability Limitation Law 2002 protects the ISP against any kind of liability for Copyright infringement. UK enacted two legislations in form of Copyright, Designs and Patents Act 1988 Digital Economy Act 2010 which imposes the obligations on ISP to notify the infringement to its subscribers, also liable to take technical measures to terminate the Internet services after reporting of infringement.

The countries also make the provisions for the penalties for offences relating to the infringement of copyright or unauthorized access of information by various ISP's or Intermediaries. The quantum of punishment is differed in every country according to the nature of offence.

Cyber Violence Against Children: A Challenge For Law Enforcement Agencies

Palvi Mathavan ,Assistant Professor, K.C. Law College,
Jammu, Research Scholar, Department Of Law, University Of Jammu

Abstract

Violence against children is a pervasive phenomenon that knows no political, cultural, economic nor technological boundaries. The boom in information and communication technologies over recent decades has brought completely new ways of establishing and maintaining relationships, especially for children and young people. Cyber violence is basically a unique form of abuse, which is generally virtual, distanced, and anonymous in nature. They do not require face to face or physical contact but results in negative face to face consequences. It is the use of computer system to cause, facilitate, or threaten violence against individuals that results in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.

Abuse against children in cyberspace includes child sexual abuse, online solicitation of child, exposure to materials that can cause psychological harm, which leads to physical harm, or harassment and intimidation including bullying. The main focus of this paper is on the various forms of violence and harms which children and young people faces in cyber space, specifically studying Jammu region of J&K State, the analysis of which shall be done with the help of statistical data available on the subject. The paper shall also review various means by which the internet may be the source of abuse of children and its impact on their growth. It attempts to identify the children who are vulnerable to such exploitation and various legal challenges faced by law enforcement agencies, prevention strategies existing at local and international level and who are the main stakeholders which could help in preventing this menace.

Key Words: Cyber Violence, Children, Child Abuse, Cyberspace, Cyber Bullying

Legal Challenges In Cyber Laws

Ayush Saran, Cyber Law Expert

Abstract

This paper is to highlight and present the existing provisions of international and national statutes and contemporary rules or law that are aimed to provide legal protection in the cyber domain. In India, Right to Privacy is now guaranteed as a fundamental right under Article 21 of Constitution of India. Further, in case of violation of social media privacy and data protection court in India recourse to the Information Technology Act, 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2015.

As far as the legal protection is concerned there is no special law exclusively to regulate social media privacy and data protection. Information Technology Act, 2000 and its subsequent amendments acts widely deal with the broad spectrum of hardware and software solutions and various cybercrime though it's few provisions narrowly deals with the concept of online privacy and data security but such provisions are not sufficient to cover up all the aspects of Privacy and Data Security issue of Cyberspace.

Therefore, the rapidly growing threat to privacy and data security issue in social media regime demands the exclusive law to deal with social media privacy. Taking into consideration the alarming threat to individual online privacy many countries have enacted the law to combat the social media privacy and data theft. Therefore, in India also, there is an immense need for an enactment of law which exclusively deals with the regulation of data protection.

Crime Against Children In Cyber World With Special Reference To Child Pornography

Shaista Kahkeshan & Naiyla Mobin Abbasi, Research Scholar,
Department Of Law, Aligarh Muslim University, Aligarh

Abstract

The swift development of the internet and other information and communication mechanism has set up unexcelled similar chances for children and adults to learn and explore the world around them. These technologies have concurrently created a new dimension in which the sexual exploitation of children is easily bloomed. Of all the crimes being committed on the internet, child pornography appears to be the one which has serious moral implications and it is the form of information that has increased in economic value in our network environment. Child pornography is any kind of representation of sexually explicit or obscene images of a minor below 18 years old. While other cyber crimes threaten the very credibility of the internet, cyber pornography promotes the use of internet. Child pornography as different from mainstream pornography is somehow connected with social issues and so receives stringent legal treatment. However, child pornography is a multi-jurisdictional problem which demands a global response. Thus, this paper analyses the very notion of Child pornography, its impact, and the legal challenges of child pornography in the Cyber world. This paper also studies about the Indian and International legal framework and Indian Judicial approach towards protection of Child pornography in the Cyber world.

Keywords: Cyber world, Child pornography, Sexual exploitation, Technology.

Cyber-Crime Against Women

Aastha Tyagi & ,Bharti Bhatt, Student,
B.B.A.L.L.B. 3RD Year, Banasthali Vidyapith, Rajasthan

Abstract

The Internet world has now become the key to gather required information, fastest communication and sharing tool, thus, making it the most valuable source. Numerous technological advancements have taken place over the last two decades and with these technological advancements the cyber-crime has also widened its roots in all directions. The crime against women is also rising in all fields whether it be crime using internet i.e. cyber-crime or sexual offences or any other offences. With the help of this paper, I plan to discuss what cyber-crime is, various types of cyber-crimes, its causes and how they have affected the women. I would also like to elaborate upon the recent increase in cyber-crime. I also plan to briefly discuss upon the various laws related to cyber-crime to protect women such as The Information Technology Act (2000) and the new laws coming up such as Criminal Amendment Act (2013). In the conclusion I plan to suggest several remedies to counter the increasing rate of cyber-crime against women.

Cyberstalking: A Clear and Present Danger

Akshay Bhardwaj, Anu Gaur, ,Minakshi Bhardwaj
University Institute Of Information Technology,
HP University, Summerhill, Shimla 171005.

Abstract

Cyberstalking is your internet variant of and can be an extension of offline stalking. The action is really to “frighten, alarm, and mentally abuse someone else." Perpetrators some times illegally accessed information to find out more regarding their targets and utilize the information that is publicly accessible networking accounts. The perpetrators can spread rumors and misinformation to discredit or intimidate them.No matter methods that are employed or used, cyberstalking is an online crime that disrupts lives, instills fear, of course, if obtained offline may result in the assault into the targeted victim. The increase of the Internet, a significant number of social networking internet sites, and the proliferation of information available on the web create new arenas that cyberstalkers use to search and terrorize their victims. Those arenas, combined with advancements to access media accounts and the Internet at large from any location, lead to a situation in harassment. This paper explores the facets that cyberstalking encompasses and the current situation in India with the legal and other recourses that are available in the country at the moment.

Keywords- cyber, stalking, law, crime, India.

RETHINKING INTERMEDIARY LIABILITIES FOR COPYRIGHT INFRINGEMENT IN DIGITAL SPACE

Debmita Mondal, Assistant Professor,
Hidayatullah National Law University, Raipur (Chhattisgarh)

ABSTRACT

Internet is posing an old challenge with newer vigour these to copyright regime across the world. While traditional copyright laws have always been questioned about the balance between protection for copyright holder and accessibility to works by public or third parties, internet has increased accessibility to content manifold and through many means.

Governments are concerned how to regulate illegal content sharing and on whom to fix the responsibility as well as the liability to check contents being shared and made accessible on online market. The technological leaps have often been reason behind the evolution of copyright law. It is technology that has also facilitated protection of copyright like digital rights management tools, anti-circumvention technologies etc.…

While there are stakeholders (including copyright holders) lobbying governments on several grounds like indecent content, illegal content or content in violation of copyright to held the facilitator like online platforms responsible for providing access such contents, there are equally strong intermediaries like Google, Face book who argue their liability starts only after being put to notice and its excruciating to scan through millions of third-party contents before posting them online. Governments across the globe including India are trying to modernize rules to meet the challenges of digital age. This paper aims at examining the concept of intermediary liability as under the Indian law and whether shifting the burden on intermediaries through mandatory technological measures like upload filters are plausible solutions for Indian Copyright regime.

Keywords: Upload Filters, Digital Network, Copyright, Intermediaries

Cyber Crime Against Women In India: Emerging Challenges

Gurpreet Kaur ,Ph.D. Scholar,
University Of Delhi

Abstract

Cybercrime implies any illegal activity that makes a use of a computer as its primary mean of commission. This offence can be committed against any individual with a criminal motive to intentionally harm the reputation of the victim or cause physical and mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet.

Crime against women is increasing day by day and cyber crime can be the most traumatic experience. Women especially young girls inexperienced in cyber world, who have been newly introduced to the internet and fail to understand the vices of internet, and hence are most susceptible to falling into the bait of cyber criminals & bullies, Cybercrimes

This paper will start by defining the cyber crime and it will go on and cover the various types of the cyber crimes that can be inflicted upon women. The paper will also discuss all the laws that are existing to protect women against all these crimes. The adequacy of these laws will also be examined by taking up some cases related to cyber crime.

The last part of the paper will suggest the measures to counter the ever increasing cybercrimes against women in India.

Keywords: cyber crime, India, women, crime against women

Impact Of Modern Cyber Communication System In Facilitating Crime And Terrorist Activities

MedhaDobhal & Veena T.S, Law Students,
Siddhartha Law College, Dehradun

Abstract

The exponential growth of Internet brought a significant impact in the field of technological developments. The worldwide connectivity of internet gave platform to the millions of people to globally communicate, access the information and get connected with several computer

systems at the same time. This global communication system on the contrary has also awakened the darker side of cyberspace by opening a new frontier for crime and terrorist activities. This privacy vulnerable network is increasingly being used by individuals or terrorist groups to attack computer networks, extract and process the information and threaten large public, specific groups or religious communities, governments by instigating violence and destroying critical networks to obtain an unfair political or ideological advantage. This paper seeks to understand how modern cyber communication system has expanded the boundaries of crime and terrorism.

Data Protection A Thinly Disguised Veil

Mike Ruban. & Arun Vignesh. T G,
B. Com LL. B (Hons) 5th Year, School of Excellence in Law,
The Tamil Nadu Dr. Ambedkar Law University.

Abstract

In the modern-day society information and data is spread on all fronts. Technology is taking over everything manual. Every information and data collected is being uploaded into the internet. Conveyance and storage of information is becoming more and more fragile. Though there are various advantages to the usage of internet and online applications. Gone are the times when information and data was an unknown quantity and was not easily available.

Since the dawn of the technological age there has also been various technological threats that have arisen. Data breaches and information breaches are becoming very imminent. Since the internet requires our information for verification it has led to various threats that intend to steal and procure other data. We often tend to take the terms and conditions of any site or application very liberally.

In the modern-day society data and information has high commercial value to various parties. The data we provide ranges from our location to interests to day to day activities. Therefore, the authors intend to look into the cases of Cambridge Analytica, Facebook and Google ads as the prima facie of our paper. The authors plan to analyse the cyber law of our country and how far does it protect data security and prevent exploitation of data and information.

Victimisation Of Women In The Internet Era: A Critical Study

Priyanka Dhar, Anindhya Tiwari ,
Hidayatullah National Law University, Raipur

Abstract

Explicit content exploits young people and impacts women severely in many cases. The global access of internet though has opened flood gates of knowledge to people but it cannot be ignored that it has brought with itself series of serious concerns which governments globally are trying to tackle. Since people today have a very easy access to pornographic materials, the major issue that concerns the government is place restrictions in such a way that minors are prevented from having access to such adult content. The major discussion that take place are focused on the roles that parents, communities, technology and laws should play in order to protect children from cyberspace obscene and pornographic threats. But the impact of such cyberspace obscene and pornographic material has to be considered in a

broader perspective with the impact it might have on the life of women who face abuse due to such content. Unfortunately the law makers and legislators hardly take cognizance of the matter even though there have been numerous researches available explaining the negative impact consumption of pornography by a spouse/partner in any household had on the physical and mental wellbeing of the other.

The paper offers an insight into how pornography and adult content victimizes women and the significant litigations and laws in various countries to prevent excessive consumption of pornography on the Internet.

Keywords: Pornography, Adult content, Internet, Cyber Pornography, Women, Victimization.

Cyber Bullying: A New Species Of User Generated Content Crime On Social Networking Websites

Bhavna Rajput, Research Scholar,
Faculty Of Law ,University Of Delhi

Abstract

Social networking websites have transformed the way we interact to each other, now everyone is publisher and broadcaster of its own information. It is true that it provides the exposure and creates myriad opportunity to everyone. At the same time it also has an ugly face that frightens everyone and poses several risk of cybercrime. Cyber bullying is one of the cybercrime that accelerated by the social networking websites. Cyber bullying is intentional repeated behaviour causing by the help of information technology to tease, humiliating, intimidating, or diminish the reputation of person. Cyber bullying does not have any legal or universally accepted definition, some scholar say that it is limited to the minors or some argue that it is not limited to any particular age group. It is also use overlapping and interchangeably with cyber stalking, and harassment. It is a new emerging cybercrime and has subject of major concern all across the globe. India does not have any legislation to penalize the crime of cyber bullying. The paper aims to discuss the concept of cyber bullying and how it is different from cyber stalking, cyber harassment, and trolling. It focuses how social networking websites has become gateway to cyber bullying. This paper also analyse legal provisions and remedies under Information Technology Act and other criminal statute. The main objective of the paper is to emphasize the emergence of define the cyber bullying and formulation of specific legal framework to criminalize it.

Bots: An Efficient Trooper Of Cybercrimes

Tushar Pathak & Divya ,Sharma Students,
Chandigarh University

Abstract

Bots are the biggest player in the cyberspace. Their use nowadays is quite common amongst people who use social media, people who play online games etc. in layman terms they are internet robots that are used to run automated tasks that are simple, repetitive and time consuming for humans. Often people pretend to have identified a bot but it’s not that easy to spot one while it is used. They are now used in almost every internet service that people use daily. The most dangerous use of it is for cyber-attacks because most of the attacks are done by well co-ordinate data transfer which makes the server or service inoperable which gives

time to hackers to steal the data or malfunction it, either way, it amounts to loss of revenue and then countless hours of repairing to bring the services back on track. The other perpetrator is social bot or socbot. It is used in the social media website to influence general opinion. It creates multiple false accounts and shares a string of posts that are made to shake or muddle with the basic thinking of a human and flood it with distorted facts. Today anyone can buy thousands of social media accounts made by bot software which are today being used in elections and to woo people for personal gains. This research paper highlights the role of bots in cybercrimes and frauds as well as discusses various preventive measures against it.

Privacy, Defamation And Dat Protection In Cyber Crime And Cyber Law

Mohit Bansal &,Prakriti Kashyap 3rd Sem B.A;LLB
(Hons School Of Law,Bahra University , Himachal Pradesh

Abstract

This paper refers to privacy, defamation and data protection in cyber-crime. With the enhancement of technology, a new category of crimes were introduced i.e. cyber-crime. In the year of 2000 Information technology Act was passed which deals with the cyber-crime and electronic commerce in India,.With a large amount of spread of internet in the entire world it has also faced a new type of crime and a new medium to commit a crime which creates a great bad impact at individual level or a group the privacy and security of a person are in danger by the internet. Right to privacy is a human right so to protect these right the different government of different nations introduced different legal framework like DPA(Data Protection Act 1988) and UK ECPA(Electronic communication privacy Act of 1986)but India does not include any legal framework which deals with private issues. Privacy are may be of many types such as privacy of a person, Privacy of personal behavior,privacy of personal communication, privacy of personal data and so on. Internet privacy is the privacy and security level of personal data published via the internet. Now a day's people also defame the another's reputation by the help of computers or internet by uploading the defamatory statement. They publish the defamatory statement on a websites or send e-mails to the other person for satisfying their personal satisfaction. The cyber-crime also creates a impact on the economy of a country depending upon the information published and the victim against whom the information has been published.

Keywords:- Privacy, defamation, security,

Crimes Against Women Under Cyber Laws

Surbhi Jain, Student BBA.LLB.(Hons) 3rd Year

Abstract

In the current era of online processing, maximum of the information is online and prone to cyber threats. This threats the woman at most. The expression 'cyber crime' cannot be restricted only to hacking or planting computer virus into another's computer, but encompasses a wide range of crimes that use information technology in their commission or preparation or harassing woman. Therefore, the subject of cyber crimes, electronic evidence and investigation of such crimes, is significantly relevant, contemporary . It deals with challenging and interesting legal issues with respect to cyber crimes that confront criminal justice systems across the world, with problems of determining jurisdiction, cross border investigation, collection of evidence, and ultimately the prosecution of the offenders.

Cyber attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense, low reputation etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Hence lays the significance of formulating an appropriate legal approach and strategies to effectively tackle the menace of cyber crimes such as hacking harassment, staking, and cyber fraud etc. Therefore, the thought provides the understanding of cyber crimes and their impacts over society with the future trends of cyber crimes.

Keywords: Cyber Attacks, Cyber Crimes ,cyber law, Consumer trust, National Security.

Responding To Cyber Crime: Need For An Interdisciplinary Approach

Miss. Ritu Panta Phd Scholar
National Law University Shimla (H.P)

Abstract

In the latest years there has been a spectacular growth in cyber crimes. The reason for this is the exponential growth in cyber space. Such a phenomenal growth in access to information on the one hand empowers the individuals and organizations and, on the other hand poses a threat to the national security as well as the individuals. Of the various factors recognized as the causes of cyber crime, the author through this paper attempts to analyze other factors such as, lack of cyber crime awareness, lack of ethical values in society and the existence of particular belief systems, as the prime contributory causes of cyber crime. Despite the legislation on cyber crime, there is seen a spurt in the cyber crimes. The primary object of the paper is to deeply analyze the subject matter of cyber crime, to enable the readers understand the serious implications it has on the national security as well as on the individuals and to enlighten them with the explicit fact, that mere legislation by itself cannot check the growing menace of cyber crimes in society. To prevent and completely stem out the commission of such crimes, it is pertinent to clearly understand the crime schemes in the cyber space, internet trends, behaviour of cyber criminals and their methods of commission of such crimes. For this extensive involvement of sociologists, academicians, politicians, educational institutions and technocrats is needed. Therefore education should be seriously involved in fight against the plague of cyber crimes. Mere surveillance by government agencies and enactment of laws will not solve the global problem of cyber crimes. Cyber crimes mainly being techno based crimes evolve with the growth in technology. Through this paper it is strongly recommended that the governmental policies and the laws enacted for tackling the scourge of such crimes must keep pace with the advancement in the field of information technology, so that effective measures to curb the spread of cyber crime could be undertaken. Further, the paper will discuss various kinds of cyber crimes. The paper will conclude with a strong recommendation and appeal to the readers, governmental and non-governmental organizations, to view the issue of cyber crimes not just from a legal prism but from a multitude of angles so that interdisciplinary approach could be adopted to effectively arrest the l problem of cyber crimes which is global in its very nature.

Cyber Security Laws And Policies In India: A Critique

Dr. Neempiya Nag, Assistant Professor,
Himachal Institute Of Legal Studies, Shahpur, Dist. Kangra, H.P.

Abstract

With the advent of twenty first century the area which has grown the most is the Information and technology. It has proved to be a boom in many aspects of day to day life ranging from telecommunications, banking, intellectual properties, medical acre ,education ,storing and dissemination of information, scientific discoveries, entertainment, construction and any other activity which we can think about which makes our life easy and comfortable. But the disadvantages have not been any lesser of the ever expanding ambit of cyber world. The world is on the verge of explosion of over information and misinformation causing all kinds of crimes related to cyber world ranging from breach of privacy, terrorism, cheating, pornography, misusing information etc. With the growth of social networking sites and easy and cheap availability of internet facilities the face and action of information has undergone a transformation posing serious threat to the social and moral value which is evident from ever increasing number of sexual crimes against women and children. Although cyber security laws to govern the ever expanding cybercrimes are covered under Information Technology Act, 2000, Rules, Indian Penal Code, Laws on Intellectual Property etc. But their enforcement and rapid updation needs to be analysed. The present paper aims to bring some light on the existing legal framework to protect the cybercrimes its implications, efficiency, applicability as well as to cover new areas and to examine what is needed to make it in compliance with other countries. This paper presents a critical commentary on the Cyber security laws in India in detail and other counties in brief.

Cyber Voyeurism: An End Of Privacy

Rishu Mala, Research Scholar,
Deptt. Of Laws, H.P. University

Abstract

Once again technology become the bane!

From time immemorial it has been seen that the need to improve has led to the motivation to the person. And only this motivation has later on resulted into the development and progress of the man in the society. Among the number of these recent advancements one of the advancement is in the sector of cyber world. This cyber world is so vast, which covers countries, continents and enables one to contact with other in fraction of a seconds. Cyber world offers number of benefits to us along with certain threats; and among these one of the major threat is cyber voyeurism. History is evident of the fact that, women, have remained victims of various forms of sexual offences. Even, in the world of recent advancements in the field of science and technology, they have been targeted and have become the victims of a cyber-voyeurism through this electronic harassment. Technology on one hand can enhance individual freedom through anonymity and privacy but on the other hand it has violated the autonomy and dignity of others. The Indian Penal Code under its section 354C along with the provisions of Information Technology Act provides for laws against cyber voyeurism and protects the end of privacy of women in this sphere.

Implications of Online Child Pornography And Related Laws

Shalini Singh And Ayushi Pandey BA-LLB 3rd Year Student ,
Maharaja Sayajirao University- Faculty Of Law.

Abstract

This new era of technological advancements has given rise to various offences especially against the new age children due to the extensive exposure to internet and the social media. Internet being a vast ever changing community, everyday something new is posted online. It makes It is hard to quantify the level of children's exposure to adult content.

Child pornography is not only a national but a global menace. What consists of child pornography is publishing, transmitting obscene material of children in electronic form.

The research is a study on how the narcissist offenders use online grooming in order to contact and manipulate vulnerable children resulting in online child pornography. The research involves real life cases available on public domain and statistical data.

Objectives:

- To understand online child pornography.
- To discuss the process of online grooming.
- To focus over the mindsets of the predators/sexual offenders involved in transmitting and publishing online child pornography and its impact on the victims.
- To understand the laws, Acts, Amendments, International Treaties passed to prevent online child pornography.

Conclusion:

The excessive exposure to social media and internet to children often tend to become the go-to place for offenders and paedophiles exploiting children. Such exploitation not only affects the victim's state of mind but also reflects the narcissistic temperament of the offenders publishing and viewing such content. Every child pornographic image and act represents a crime scene in itself and the same must be addressed by law enforcement authorities along with awareness amongst the public.

Cyber Terrorism: Threats And Challenges

Karsin Manocha & Geetansh Khurana, Ba Llb(H) Ix Sem.,
Faculty Of Law, Jamia Millia Islamia, New Delhi-25
Samidha Goel, Yashasvi Anil Kumar, Student s B.A.LL.B.
University Institute of Legal Studies, Chandigarh University,

Abstract

The growing popularity of social networking sites among internet users demands an introspection of personal and social behaviour of human beings. Today, millions of people across the world have their profiles on social networking sites. Everything appears nice when you create a profile on social networking sites, but how do you feel when someone starts blackmailing using your data. Constant violation of regulations related to social networking has resulted in civil and criminal cases that need urgent attention. Major example of hindering the right to privacy of social media users is Facebook-Cambridge Analytica Data Scandal, where the most used social networking site leaked personal data of around 87 million of its users to Cambridge Analytica in 2015, for US Presidential Elections; then in 2016, for Brexit voting; and again, in early 2018 for Mexican general elections. Recently,

Snapchat was in the controversy for the main hub of child pornography predators.The laws that regulate social networking sites are more than 17 years old, while Facebook and other popular social media websites are just 15 years old or less. Social networking sites become a reason for anxiety and addiction. It starts affecting personal relationships with friends, spouse and family members. These sites make private life and public life of an individual, a digital document. This research study tries to explore all these crimes of social networking sites on its users and the criminal mindset behind these sorts of hinderance of privacy and other crimes relating to social networking sites.

Key words – Social networking sites, Personal privacy, Cyber infidelity, Cyber-crime.

Can Social Media And Cyber Security Go Hand In Hand?

Dr. Sanyogita Asstt. Prof., UILS, HPU, Chaura Maidaan, Shimla.
Dr. Bhavana Sharma Principal, HIMCAPES; College of Law,
Badhera, Haroli, Una,H.P.

Abstract

The issue of cyber crimes has received much attention of late, as individual and organizational losses from online crimes frequently reach into the hundreds of thousands or even millions of dollars per incident. Computer criminals have begun deploying advanced, distributed techniques, which are increasingly effective and devastating. This paper describes a number of these techniques and details one particularly prevalent trend: the employment of large networks of compromised computers, or bonnets, to conduct a wide variety of online crimes. The paper also relates a number of the practical, legal, and ethical challenges experienced by practitioners ,law enforcement, and researchers who must deal with these emergent threats. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords—Cloud Computing & Law, Cyber Law, Cyber Security, Mobile Law

Cyber Law and Cyber Crimes: Issues and Challenges

Samidha Goe,l Yashasvi ,Anil Kumar Student,
B.A.LL.B,University Institute of Legal Studies, Chandigarh University.

. **Abstract**

The growing popularity of social networking sites among internet users demands an introspection of personal and social behaviour of human beings. Today, millions of people across the world have their profiles on social networking sites. Everything appears nice when you create a profile on social networking sites, but how do you feel when someone starts blackmailing using your data. Constant violation of regulations related to social networking has resulted in civil and criminal cases that need urgent attention. Major example of hindering the right to privacy of social media users is Facebook-Cambridge Analytica Data Scandal, where the most used social networking site leaked personal data of around 87 million of its users to Cambridge Analytica in 2015, for US Presidential Elections; then in 2016, for Brexit voting; and again, in early 2018 for Mexican general elections. Recently, Snapchat was in the controversy for the main hub of child pornography predators. The laws that regulate social networking sites are more than 17 years old, while Facebook and other

popular social media websites are just 15 years old or less. Social networking sites become a reason for anxiety and addiction. It starts affecting personal relationships with friends, spouse and family members. These sites make private life and public life of an individual, a digital document. This research study tries to explore all these crimes of social networking sites on its users and the criminal mindset behind these sorts of hinderance of privacy and other crimes relating to social networking sites.

Key words – Social networking sites, Personal privacy, Cyber infidelity, Cyber-crime.

Crimes Against Women In Cyber Laws

Sanskriti Dave, Shruti Kakkad,
B.ALLB Hons. with specialization in Energy Laws.

Abstract

The Internet is one of the fastest-growing areas of technical infrastructure development in all nations. In the current era of online processing, maximum of the critical information and details are online and prone to cyber threats. The world of internet provides every user all the required information fastest communication and sharing tool making it the most valuable source of information. The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances. Cyber- crime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole. Cyber-crimes committed against persons include various crimes like transmission of obscene messages, harassment of any one with the use of a computer such as e-mail, cyber-bullying and cyber-stalking.

In India where the society looks down upon the women, and the law doesn't even properly recognize cybercrimes. In India the term "cybercrime against women" includes sexual crimes and sexual abuses on the internet. Cyber-crime is emerging as a challenge for national and economic security.

In this paper we will discuss how women get affected or get harassed by cyber related criminal acts. Moreover we will deal with all the types of cyber crimes and majorly those related to women. The present study is an attempt to highlight the cyber crimes against women in India.

Keywords:- Cyber crime, Women, Internet, India.

Cloud Computing- The Data Overhead

Gulshan Kumar & Shashank Rai,
Students, Lovely Professional University

Abstract

Nature cloud holds water, the Internet cloud holds mammoth amount of data. Cloud computing is a term borrowed from science to explain the type of infrastructure which is cohesive and unified, which is widely accessible and which covers a large area just like the cloud in the sky spreads over a big zone and showers multiple benefits. It is all about resource sharing and free and easy accessibility directly to the nebula of the computers which provide trillions of data. The ultimate ends of any service are the consumers. Thus, it is the user or the consumer which consummates the entire goal of cloud computing. Cloud computing can be divided into following four categories, private cloud, public cloud, hybrid cloud and community cloud. Development of cloud computing is accompanied by legal issues. Though presently, it is the fastest growing segment of the industry yet the consumers are still reluctant

to deploy business in the cloud. No matter how careful you are with your personal data, by subscribing to the cloud you will be giving up some control to an external source. The pivotal role in securing data is to be mainly played by the cooperation and mutual trust of the service provider and the infrastructure provider. Now the question is who will be held liable for the data leakage? The Author will also try to draw the attention towards cloud computing, advantages and disadvantages and legal approach towards the same, as the infringements and the cyber crime being committed in the cloud also need legal control.

Data Rights, Ethics And Its Relevancy In The Current Scenario

Mudit Verma, & Samayak Jain,
Hidayatullah National Law University, Atal Nagar

Abstract

In today's world, privacy is a big concern and when it includes cyber data, the concern becomes much bigger. This paper aims in reflecting the importance of data ethics and data rights, the risk which is associated with it in the near future and how can we maintain our privacy.

The paper has been divided into four chapters; they being the research questions as well. The first question is regarding the scope of the topic and it has been adequately dealt with around the world and not only confined to a particular place. It is not exclusive in nature. What is the importance of data ethics and data rights, this makes up our second question and it is submitted that data rights should be treated within the scope of human rights. The third problem that arises is the risk posed by the third entity and digital platforms like Facebook, TikTok, Reddit, Twitter, etc. It has discussed the infamous Cambridge Analytica case. The paper has also discussed how data can be used as a weapon against each and every person. The last question deals with the solutions and precautions of the risks associated with the data and the paper deals with both ethical and legal solutions, from awareness to the user-friendly terms and conditions.

It is concluded that data rights also come under the ambit of privacy and human rights and it is significant to understand the threats which eventually reflects the need of International Cyber Space Laws and Regulations.

Keywords: Data Ethics; Privacy; Human Rights; Cambridge Analytica; International Regulations

Crime Against Women An Explatory Study On Online Harassment: Cyber Stalking

Siddhant Kumar Das & Saransh Sahu (BBA LLB)(H) Third-Year ,
Lovely Professional University, Phagwara, Punjab

Abstract

"YATRA NARYANTU PUJYATE RAMAYANTE TATRAH DEVTAH"
(WHERE WOMEN ARE RESPECTED RESIDE THE GODS)

Well!!! Sounds good? But in today's fast paced, ultra modern techno savvy world does this statement hold true?

Computers and Internet have today pervaded every sphere of human existence. However, it won't be an exaggeration to say that the boon of Computers today has taken an ugly shape in the form of cyber crimes and turned into more of a Bane.

Information technology is a double edged sword which can be used for both creative and destructive purposes. It's similar to the invention of atomic energy in the past or nuclear

energy in recent times. How we use it determines its positive or negative impact. Unfortunately, With the advent of technology, cyber crime and victimization of women are on all time high and it poses a major threat to the security of a person as a whole. The new cyber crime of cyber-violence against women, including cyber stalking, e-mail harassment and using internet to publish obscene information to exploit or embarrass women is taking alarming proportions. Studies have shown that about 60 per cent of all websites have sexual content. 25 per cent of them solicit their visitors. To mention here, Cyber pornography is believed to be one of the largest businesses on the internet today. Millions of pornographic websites bear testimony to this.

Cyber stalking has become one of the most popular internet crime in the modern world. Cyber stalking is the term is used in this report to refer to the use of the Internet other electronic communications devices to stalk another person. Stalking generally involvesmentally harassing or threatening an individual such as following a woman, specially at her home or place of business, making phone calls, leaving written messages or vandalizing a person's property. While some conduct involve menacing behavior such behavior may be a prelude to stalking and violence and should betreated seriously. According to a Survey, 60 percent of cyber stalking victims are women. Thus it now becomes imperative to look into the severity of cyber crime and look into methods to combat its menace.

40 percent of women have experienced dating violence via social media, posted disturbing status updates about them on Face book, or sent harassing text messages or hurtful tweets about them on Twitter. The biggest problem of cyber crime lies in the modus operandi of thecyber criminal. The police, judiciary and the investigative agencies need to stay abreast with the latest developments in web-based applications so that they can quickly identify the actual perpetrator. Governments can take legislative measures especially for rights of women's to protect them from electronic spaces.

India is considered as one of the very few countries to enact IT Act 2000 to combat cybercrimes; This Act is widely cover commercial and economic crime. Not only IT act but Indian Penal Code and Indian Constitution has also provided special provision for women's rights.

Technology is growing at a faster rate and has take away the green browers, which was introduced for a good use but now it is misused by the hacker this paper will discussed about stalking , stalkers how they affect the life of women and how they mentally harass the women and what all measures should be taken to protect women against this cyber stalking.

Cyber Violence Against Women

Siddharth Srivastav, Ankita Kar Students, 4th Year, BA-LL.B.,
Symbiosis Law School, Hyderabad ,Telangana-

Abstract

The Internet begun with the introduction of computers in 1950's but it was only commercially exploited in the late 1980's.This is the era of the new 'technological generation' where burgeon of information and communication technologies (ICT) and social networking sites (SNS) is ever rising. Many of the routine, mundane works have been made simple by the advent of the Internet.

As there has been significant magnification in the usage of digital space and it's inclusionary, so has been the amplification of crime against women with the newest of facets and urbane usage of technologies, known as cyber-violence which includes cyber-bullying, online harassment, cyber dating abuse, revenge porn, and cyber-stalking, etc. Cyber-crime has emerged as a major challenge to law enforcement agencies in the country, while women and children remain at constant risk. Offenders are gradually misusing Cyber platforms to harass and abuse women and children for voyeuristic pleasures in India.

In this paper, the researchers plan to deliberate upon the various types of crimes that are inflicted upon women and its probable causes. The researchers shall examine various laws that exist to protect women in cases relating to cyber-violence. Analysis of few landmark cases shall be done with regard to cybercrimes in given paper and conclusion be drawn thereafter.

The researchers would try to suggest several viable solutions to counter the ever increasing cybercrime against women and changes, if any, required in legal system to effectively curb the rising spirits of cyber criminals.

Key Words: Cybercrime, Cyber-violence, Women and children, Cyber-bullying.

Cyber Defamation And Meme Culture

Vanshika Agrawal & Shubhangi Sahu, Student,Semester III,
Hidayatullah National Law University, Naya Raipur, Chhattisgarh

Abstract

The varsity of Internet has not left any field untouched, be it something as simple as doing daily chores or something as complex as crimes. Crimes committed with the aid of internet are known as Cyber Crimes. On the basis of its nature, Cyber Crime is divided into two categories, Crimes on Internet, which are basically old crimes, who have just found a medium in the Internet; and Crimes of Internet, which are the new crimes created with the internet itself. In this paper, the authors attempt to deal with a crime on internet, i.e. Cyber Defamation. Defamation implies harm caused to anyone's reputation in the right thinking people of the society. And with the present scenario of social media, where it has become so easy to spread rumours anonymously, incidences of defamation have become more rampant. "Meme culture" is also a result of these advancements. "Meme Culture" connotes presenting an idea or an issue with a comic undertone. Recent trends have shown extensive use of meme to criticise and defame certain entities and sections of the society, and in some of the cases, suits have been adjudicated and damages have been awarded. In the light of these developments, it is paramount to analyse the position of India and the judicial approach in balancing freedom of speech and expression projected with memes with right to reputation guaranteed by the constitution.

Efficacy Of Child Pornography Laws In India : Safety And Security In The Cyberspace

Omkar Upadhyay Student, 2 nd year B.A.LL.B. (Hons.),
Maharashtra National Law University, Nagpur,

Abstract

About more than half of the world's population has today in one way or other interacted with the cyberspace for innumerable reasons. With technological advancements, there has been enormous increase in number of people finding solace in the cyberspace having all sorts of motives. This, apart from bringing plethora of benefits, has been a cause of serious

repercussions. The prime of them being pornography or specifically forced pornography. But this isn't all it has caused. The ultimate evil taking birth in the cyberspace is 'Child Pornography' which though sometimes is with consent but largely is an act of abuse and molestation having serious effects on the mind and psychology of a child, both a boy and a girl. Cyberspace has emerged as a safe haven for the perpetrators of this heinous crime of indulging in production, storage, transmission and browsing of child pornography. India like every other country is also a victim of this growing crime. Thus this research is aimed at assessing the efficacy of laws pertaining to child pornography such as the POCSO Act, IT Act and IPC in dealing and handling the problems and issues challenging the cyber society. While analysing the Indian legislations the authors have also taking into consideration the international conventions to which India is a party. The authors have then proceeded to present with prospective changes and amendments which could be brought in the legislations to better tackle the issue and make India free of this evil.

Crime Against Women In Cyber World (Cyber Obscenity And Victimization)

Prashant Bhardwaj And Kristen Sleeth,
Himachal Pradesh National Law University

Abstract

For every lock, there is someone out there
Trying to pick it or break it…….……..David Bernstein

From ravens to facetime, technology has experienced a great change and in this transitional phase of differentiation, mobile phones have taken an important place in man's life. Uses and misuses are two different faces of the same coin and one goes with the other with people and various turns and folds of the society. Cyber Obscenity is one of the major misuses of this technological advancement. There is a history of the relevance and meaning of the word "*obscenity*" and from ancient Greek theatres to *Regina* v *Hicklin* the first test named as Hicklin Test was established and obscenity was what reasonable men would think that will corrupt public order and morality. In India the modified version of Hicklin test was established in the case of *RanjitUdeshiv* v *State of Maharashtra*.

Section 292 of The Indian Penal Code, 1860 laid the ground for Section 67 of The Information Technology Act, 2000 as sec. 292 is considered as the offline version of sec. 67 although the punishments and the fines are differently listed. The paper attempts to study the distinction between Section 66(e) and Section 67 of The Information Technology Act, 2000. The paper also attempts to list down measures to turn upon the "Revenge Porn" and study the obscenity in respect to moral harm to the society at large.

Analysis of important cases are also been discussed in the research paper. The research is in pure doctrinal form and the data's are collected from the secondary sources availablewhich includes articles, cases, journals etc.

A Critical Study Of I.P.R Laws Governing Copyrights And Trademarks In Indian Cyber-Space Regime In The Light Of Comparable Foreign Laws"

Mr. Sumanas Dash & Mr. Aditya Mishra , 4th Year,
B.A. LL. B (Hons.), Himachal Pradesh National Law University, Shimla.

Abstract

Intellectual property rights are like any other property right. They allow creators, or owners, of patents, trademarks or copyrighted works to benefit from their own work or investment in a creation.

The unique matrix of cyberspace has produced different categories of infringements including Deep linking, Framing, Piracy of music, software and video as well as other Digital Copyrights infringements. The WIPO, through its treaty, has made important initiatives to bring harmonization in copyright regimes across various jurisdictions. Although India is not a signatory to the treaty, it is a party to the Berne Convention that protects copyrights across many countries that are its member signatories. Also, WTO initiatives led to the creation of the TRIPS Agreement, another instrument that has made several strides in protection of copyrights. India is a signatory to the TRIPS Agreement.

In India, The Copyright Act, 1957 and Trademark Act, 1999 deal with the protection of copyrights and trademarks, respectively. However, these sets of law fail to deal with the rising instances of infringements arising through the usage of the ever-growing domain of cyberspace. It may be said that the law has failed to keep pace with the changing times. As a result, Indian Courts have to seek out relevant judgments given by foreign authorities, courts and tribunals in order to deal with such matters. Thus, parallels must be drawn between Indian and Foreign IPR laws so that the loopholes in the Indian Law may be detected, and filled in.

Liability Of On Line Marketplaces For Legal Violations By E-Businesses Using Their Webspace For Selling Or Advertising– An Analysis Of Indian Legal Framework

Dr. Poonam Dass**,** Associate Professor**,**
Faculty Of Law, University Of Delhi

Abstract

Online marketplaces like Amazon, etc. act as intermediaries for selling products online. These market places not only provide space for doing business but also maintain inventory and deliver the products to the consumers and also provide advertising spaces and links to such sellers selling through their own websites. For the purpose of advertising these intermediaries sell keywords for advertising on their portals which are used as meta tags to display the advertisement or links. The keywords can be the similar or identical to the trade mark of other businesses.

The Information Technology Act exempts intermediary from third party liability so long the role is passive and it follows due diligence. Recently the Delhi HC in a case filed by Direct selling companies like Oriflame, made the online marketplaces like Amazon prima facie liable for tort of inducement of breach of contract. The sellers using their webspace were restrained from selling the products of such companies. In another case, the Google was absolved from the liability of trade mark infringement for providing keywords to its advertisers similar to the trademarks of other businesses. These developments in legal arena requires a study into the aspect of intermediary liability for legal violations by third parties in cases where there is some indirect involvement of such intermediaries and also to study whether the law in India at present is sufficient to deal with such cases or does it require amendments.

Relationship Of Cyber Law With Intellectual Property Rights

Yumna Chand & Agam Verma, Student of B.A.LL.B 4th year ,
JIMS, School Of Law, affiliated to GGSIPU

Abstract

Virtual worlds are important integral parts of today's life style. Every citizen is more used to

connect to the virtual worlds through the computers and other communicating devices. In a Cyber space, the virtual worlds have to use devices (software) that obey the CL and cyber ethics. The greatest threat of risk to software industry, engineering process and education is due to lack of future imagination and inability to understand strongest bond established between software engineering discipline and legal issues of the cyber space.

[1]The greatest threat of risk to software industry, engineering process and education is due to lack of future imagination and inability to understand strongest bond established between software engineering discipline and legal issues of the cyber space.

At present, legal system and framework are inadequate to address all the aspects of Information Technology. As and when new computing technologies walks into the life style, law has to learn the changes. A lot of grey areas exist in the legal system are billion dollar questions to the software industry and should evolve on a continuous process.

As far as non-functional and domain requirements in software development process is concerned lack of knowledge of IPR and CL could drive into cyber catastrophe resulting in misbehaving software functionalities and a loss to the society in general and serious implications on Governance, Business, Crimes, Entertainment, Information delivery, Education etc., To ensure that Software development does not violate the Cyber Laws and enforces IPR calls for paradigm shift in analyzing and modeling non-functional and domain requirements in order to deliver quality and legal Software product.

Military And Intelligence Actions In Cyberspace From Indian Perspective.

Rajalakshmi Sumathi Kothandaraman,
Student of PG Diploma in Cyber laws And Cyber forensics,
National Law School University ,Bengaluru.

Abstract

Military and intelligence actions are crucial from the point of national security in that the essential information obtained from intelligence activities helps in formulating policies for the national and international levels. The crucial data or information from different sources assist the military commanders in making tactical decisions before conducting operations.

With the advent of computers and the concept of networking which has given birth to the internet, the world has seen the emergence of a virtual space called the cyberspace which is characterized by no logical geographical boundaries.

The purpose of this study is to realise how this new digital world influences the military and intelligence activities in gathering crucial informations to design defensive mechanisms for their country . As in any research, it is imperative to recognise the impediments encountered that halt this process of investigation which would have otherwise helped reach the crucial data or information. This study also helps in recognising both the constructive and destructive trends in the digital world which in turn makes it necessary to make appropriate legal amendments in the country to ensure national security and also to facilitate national progress on all fronts. Hence, the present study will help to ascertain whether the digital world has helped the intelligence department in achieving their goal in safeguarding the national interest.

Crimes Of Social Networking Sites

P B Adithya Sai & Ashwath Ethiraj ,School Of Law,
Vels Institute Of Science, Technology & Advanced Studies(Vistas)

Abstract

It is a truth that every coin has two sides , same for internet it has both advantage and disadvantage. One of the most important disadvantage of internet is the Cyber Crime offence. The Social Networking Sites have created an era in the history of Cyber Space influencing netizens in their Personal sphere as well as professional level. The growth and impact of their websites at the exponential rate have attracted the cyber offender to commit Cyber Crimes in social medias. The Cyber offender are committing offence related to Privacy, Defamation, Misrepresentation of Identity, Obscenity and pornography, Sending offensive Messages, Cyber Terrorism and so on. In India most of the Cyber crime are committed by persons who are well equipped with cyber knowledge affecting the common internet users. In this paper tries to discussed various categories of cyber crimes which is based on social networking sites. This paper also suggested the various preventive measures against these unlawful acts in day to day life.

Keywords: Cyber Crime, Social Media, Cyber Law, Cyber Space, Legal Provision, Punishment, Preventions.

Gender Harassament Through Cyber space and its Psychological Imapcton Its Victims

Alvina Ahsan And Anas Azeem
Student National Law University Odisha

Abstract

The coming of the age of internet reduced distances to minutes but like all other things, it had a flip side to it as well. It made the boundaries across the globe to evaporate, so did it do for the crimes committed. This new era of crime requires no physical intimidation or access thus giving the criminals more power to intimidate anyone comfortably from their spaces.

Gender harassment taking place through cyberspace has violated the boundaries of individual privacy and also the right to live with dignity. Today, the most intimate moments of an individual's life is secretly being viewed upon by an unknown person virtually to creepily satisfy his/her sexual desires or misuse it to his/her benefits.

This paper discusses about the extent of gender harassment through cyberspace and how the problem is being dealt with in India. The inadequate number of cyber cells across the country compels the victims to report their cases as regular FIRs. The lack of knowledge of the regular cops in this area of crime makes cases go unaddressed properly. This paper also discusses how gender harassment through cyberspace affects the victim psychologically and the scarit imprints on their life. Being virtually abused is still a crime Indian society is not well acquainted with and the victim is judged on an uneven balance. The paper suggests solutions to address the crime positively in favor of the victims.

Analysis Of The Regulatory Framework For Prevention And Redress Of Online Banking Fraud

Mr. Arjun Malhotra (Pursuing LLM from USLLS, Dwarka, New Delhi),
Ms. Ayushi Negi (Advocate High Court of Himachal Pradesh)

Abstract

Electronic Commerce has drastically changed the landscape of world economies. The

manifold increase in online banking is mainly on account of ease and accessibility. Majority of financial transactions are being done over the internet. The Indian Government has pushed for Online Banking as a way to financial monitoring and aligning with world markets and global trends. It is necessary that banking frauds that take place over the internet are duly addressed by suitable statutory and regulatory framework. It is the prime responsibility of the Banking Regulatory body to provide a framework to prevent frauds.

Regulatory Framework must at least perform two set of functions. Firstly it should ensure robust security to be implemented by Banks and Financial Institutions in their operations and secondly it must mandate for a mechanism to redress online banking frauds. The online banking fraud involves extreme level of technical competence as such its investigation should have requisite expertise. The redress framework must be consumer centric to prevent innocent consumers who have acted reasonably from any financial harms or prejudices.

This Paper is doctrinal in nature and shall analyze the Legal challenges of online Banking such as information security and preventing unauthorized transactions, followed by the present regulatory mechanism, the regulatory guidelines issued by the Reserve Bank of India and its compliance by 3 major banks namely CITI Bank, HDFC Bank and State Bank of India , while formulating their anti-fraud policies for online operations.

Changing Pattern Of Criminal Economy: Use Of Cryptocurrencies In Darknet And Criminal Forums

Riddhi Pratim Dutta Ph.D. Researcher. NUJS, Kolkata.

Abstract

Tracking money is the first thing police do while trying to crack any crime. So, obfuscation of monetary trail is an essential priority for any criminal Problem was using traditional financial institutions leave a paper trail that can't be erased completely. Satoshi Nakamoto, while disgruntled with current economic structure offered a monetary system which is not depended on Central banks nor uses traditional financial intermediaries like banks to transfer value. While the system was conceived for common people, the anonymity offered by cryptocurrencies became heaven sent gift for criminals. Within a few years criminals ditched traditional fiat currencies and preferred to be paid in anonymous cryptocurrencies like Bitcoin. Problem is Bitcoin is hugely volatile and later criminals realized it does not offer as much privacy as was thought before.

This paper discusses the history of crypto currencies and why anonymity was incorporated in them. We discuss Silk Road, a notorious drug and crime marketplace and how they managed to tackle volatility of virtual coins and managed to make it preferred currency of criminals. Cryptocurrencies facilitated crimes ranging from money laundering to drug sale. We will examine how businesses and criminals thrived in the darknet using Bitcoin and how they expanded their empire. Then we will discuss legal response and how police are also using the same anonymity to counter the new challenge. We will conclude by showing how this new method of transaction is a fluid system and banning them doesn't work in real life.

Cyber Security- Advanced Technological Threat

Shailja Dhyani ,Neeta Rawat,
Student BBA LLB (Hons) Graphic Era Hill University, Dehradun

Abstract

With time area of cyber security is increased. It has very wide scope. Earlier if a person wants

to harm someone, he needs to come near him. But now with technological advancement a person sitting far away can harm you. Now cyber crimes are gaining worldwide attention. Cyber security has become a major concern in the world. We hear cyber attacks continuously on someone's bank account, social sites, computer (secret information) etc. The expenditure on cyber security is increasing year by year. There are many companies which are offering security solutions but these solutions do little to protect from cyber attacks. Cyber security protects the data and integrity of computing assets belonging to or connecting to an organization's network. Our most of the time is spent on internet. Nowadays everyone has access to internet so the threat becomes bigger.

In this technology era we need advanced experts to protect us from frequent cyber attacks. The worst part of cyber attack is that it can be done from anywhere in the world. In this no physical appearance is required. Most of the cyber attackers attempt to attack on website or a server instead a network as it is easier for them. Large business houses have complained of security beaches. There are different methods to protect data from cyber attackers. This paper focuses on cyber crimes, cyber security and challenges faced by cyber security. In this paper we will discuss how the trend of cyber crime is emerging and secure internet. We will also categorize the threats and discuss protection mechanisms.

Copyright Infringement On The Internet In India

Anahida bhardwaj, Fourth year law student of Symbiosis Law School, NOIDA, constituent of Symbiosis International (Deemed) University, Pune

Abstract

Copyright infringement has been a severe problem that has plagued our modern society. With the expansion of the digital sphere, it is even more difficult to track instances of infringement and seek remedies. With the Internet the battle seems to be lost, since it allows the access to an enormous quantity of information anytime, anyplace without any constraints. The Internet has often been referred to as one large copy machine that can make and distribute an unlimited number of copies of content worldwide. Said to be one of the most poignant inventions of modern man, it has led to the creation of another sphere wherein infringement of intellectual property rights is rampant and difficult to track down. With the element of anonymity over the internet, any breach of intellectual property rights would be difficult to track down to the perpetrator of the offence. The ease with which infringement could take place could potentially become the reason over which individuals may not want to share their work over the Internet, thereby denying the opportunity to several individuals to have access to useful information. This paper deals with the existing regime of copyright laws as applied in India and the potential reforms that could be undertaken to prevent the copyright infringement over the Internet

A Comparative Analysis Of Crime Against Women In India And Usa In Virtual Reality

Sneha Maji Terence , Akansha Bansal Student, Amity Law School, Noida, BBA-LLB(H)

Abstract

Morris states, "Crime is what the society says a crime by establishing that an act is a violation of criminal law. Without law there can be no crime at all although there will be moral indignation which results in law being enacted", thus committing such an act in the digital

platform will amount to cyber crime. Cyber crime has two dimensions-one, commission of an act by unlawful alteration of data in information technology, secondly commission of obscene act, stalking, pornography, voyeurism, etc that lowers the reputation of victim, cyber crime against women mostly revolves around the second categories mentioned above.

The U.S. Department of Justice statistics suggested that 850,000 American adults mostly women are targets of cyber-stalking each year, and 40 percent of women have experienced dating violence delivered electronically. The number of cyber crimes in India in 2014 and 2015 have been 9622 and 11592 respectively. The research paper covers different dimensions of cyber crime faced by women in the virtual reality and the statutory regulation to combat the situations. Major Cyber threats and heinous form of cyber crime against women in Indian and American context have also been discussed in the paper. The major reasons for failure of criminal justice system to deal with cyber crime effectively have been discussed in the paper and the paper also lights on the issue of harassments faced by the victims in the hand of delegated authorities.

Keynotes- virtual reality, cyber crime, voyeurism, obscenity.

Crimes Affecting Governmenl Bodies In Cyberspace: Challenges And Solutions

Anshuman Srivastava, Mohd. Altmash And
Aamir Raza Khan Students,Jamia Mellia Islamia

Abstract

The society which exists these days has got its foundation from the ongoing development which takes place constantly and one of thesis of cyberspace, which is nothing but a chain of communication in an isolated computer network space. A by-product of cyberspace is cybercrime that either targets computer network through internet or use it as a helping hand in committing various kinds of network scams like cyber-squatting, phishing, vishing etc. Cybercrimes are host to several other degrading factors which result in a complete meltdown of the society, it leads to financial downfall, complete subjugation of intellectual properties, makes people lose their inner belief and confidence which leads to their self-destruction and personality deterioration.

Every society needs a stable organization which can handle all the upheavals occurring at the place, but due to the interference of cybercrimes this process becomes difficult to execute. Cyber related crimes make a government body lose its authenticity and supremacy, these acts lead to heavy monetary loses and results in severe security and moral threats for the peoples cohabitating in that society. Some of the major cyber threats which revolve around the governmental bodies are cyber terrorism, child pornography, cyber trafficking and the list goes on. There are also some preventive measures which can be introduced by the concerned authorities to handle the repercussions like highly secured passwords, security encrypted tools, anti-virus software's and many more.

Crimes Against Women In Cyber World

Vijay Sri.E.R, BBA LLB Hon),VIT School Of Law, Vit Campus, Channai

Abstract

The traditional Indian society places women in a very high regards the Vedas glorified women as the mother, the creator one who gives life and worshipped her as a goddess. The women occupied a vital role and as such her subjugation and mistreatment were looked upon

as demeaning to not only the women but towards the whole society. However, in modern times women are viewed and portrayed as a sex object, she is treated inferior to men in various societal spheres and functions, this had created a huge gender bias between the men and women where even the men think that their wrongdoings towards women cannot be penalised. Cyber crime and internet bullying works in a similar way where the wrong doers are not afraid of any authority that can penalise. The issues involved in cybercrimes are like adult bullying, cyber stalking, hacking, defamation, morphed pornographic images, and electronic blackmailing. The persons committing these crimes and also the other crimes related to this are for many reasons, are unlikely to be identified or punished. Through this paper we can get a better understanding of cyber victimization and discover how to improve responses to cybercrimes against women.

KEY WORDS: women victimization, cyber crimes.

Cyber Crime Against Women In India

Ashish Tiwari ,Law Student 3rd Year B.A L.L.B (Hons)
Amity University Lucknow Campus

Abstract

Internet in 1990s was a luxury. Today it has become so readily available that even a poor person running a tea stall owns it. Internet connects people from all part of the world. They share their thoughts, ideas and opinions with each other but readily availability of technology has added a dangerous significance to traditional crimes. Women has always been the victims of these traditional crime such as rape, voyeurism, sexual harassment, stalking etc. The availability of technology so easily has made such crimes more dangerous. Now the criminal can easily records the footage of a rape scene and can extort money to publish the private video photos on the internet. Such rampant misuse of technology not only harms her physical state but also her mental state. Therefore, the author has discussed issues such as cyber stalking, cyber harassment and all such problems related to cyber-crime against women in India. The author has covered all the legal aspects and has provided practical solution to it.

Keywords – Cyber-crime, Women, Internet, Traditional crimes.

Cyber Crime On Social Networking Sites

Vani, Student , Banasthali University ,Haryana

Abstract

Same like the moulds Cyber Space has spread his feet all around within this World since 1997 when social network come into this picture. With this superhighway whether the person is willing or unwilling, direct or indirect they are connected. Internet is similar to a coin having two sides, whose positive and negative impact are touching lives of each and every human being of this world. The illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them is termed as Cyber Crime. It can take place without physical involvement. The positive effect of internet, it provides information of anything at any part in this world. Internet also exhibits wider negative effects which are mainly faced by women, child and old age people. There are the common form of Cyber-Crime which can be arisen easily such as Cyber Pornography, Cyber Stalking, Blackmailing, Online Trolling, morphing and many others. But there are Cyber laws which are recently been enacted in 2000 The Information Technology Act and with the

progressive amendments in this field. The main purpose of this paper is to put awareness among the Homo sapiens about this problem and to put forward the absolute reason for the constrained success of this problem. The Cyber Crime has both its boon and bane which totally depend on the use of this Super Highway of the 21st Century. By providing secure Cyber eco-system the number of cyber crime can be reduced.

Keywords: Internet, Cyber-Crime, Cyber pornography, Cyber stalking, Information Technology Act, Cyber-eco system.

Cyber Crimes And Law In India: A Critical Analysis

Raj Kumar Garg, Research Scholar H.P. University,And
Susheela, BALLB 5th Sem., Indian Institute Of Legal Studies, HPNLU, Shimla.

Abstract

World is passing through the unprecedented phase of metamorphosis in the area of information technology, that has made dramatic changes in the daily routine of our life .With the development of Science and Technology human beings all over the world live a comfort life and conveniently enjoy fruits of its. In the cyberspace there is net of websites and they are busy day and night in disseminating useful information but it has generated some problems also. A number of frauds are committed with the help of these websites. People are cheated by the use of information technology and the security of electronic record is at stake. The problem of developed countries is more acute than the problems of developing countries, because more the advancement more are the chances of its misuse. Law violators are always like to go one step ahead from law makers. It is not exaggeration to say that before the enforcement of law, culprit chalk out the strategy to violate it and the cyber law is not exceptions to it. WTO and other international organisations having concerned with international trade are worried for the misuse of Information Technology and realised that some uniform and concrete steps may be taken at International and national levels to regulate the Electronic Commerce. In India also passed an act known as Information Technology Act in the year 2000to regulate the cyber activities and to curb cyber crime. This paper deals with cyber crimes in India and law and policies to regulate theses crimes.

Expension Of Cyber Terrorism In India: A Physical Reality Or Digital Myth

Dr. Shiv Raman And Ms. Nidhi Sharma Assistant Professor (Law)
Amity Law School, Amity University, Gurgaon

Abstract

Cyber terrorism is a global issue which is one of the most ignored & underestimated issue considered in India. India has the maximum internet users, called as ‘Netizens’ after USA and China. The over dependency over the internet increase the vulnerabilities & transformed theiraggressions into feeling of revenge, which turned them criminals, Cyber warriors and hostility to the country. Most of the Indian citizens are insensitive towards cyber threats of being victimized of virtual world. The information technology has opened the ocean of opportunities to the world for development of their financial infrastructures. The Cybercrimes are increasing every moment. The netizens are ignorant and of state of mind that their activities are unnoticed. We generally share our significant & super sensitive data & information unintentionally on social media. The momentous growth of Cyber world posed the threats of Cyber terrorism. The Cyber-attacks has tendency of depictionof lethal, non-

lethal psychological well-being, public confidence & political attitudes. Generally, it is to consider as Cyber terrorism affects only the national security system. But infect- it also affects their psyche & cognition. The Cyber terrorist expanded growth of Cyber-attacks, which is dramatically increased in past few years. It has caused mass destruction & damage to nuclear facilities & critical command & control system. The Cyber experts are working to strengthen more and more capacity to restrain Cyber-attacks over Govt. system, defense websites, financial and banking system and most important nuclear facilities.

Key Words: Netizen, Cyber warriors, Cyber victimization, Cyber threats and Cyber-attacks.

Cyber Crime: The Faceless Criminals

Harleen Kaur Rait,Akanksha Sahoo, BBA.LLB student ,
Symbiosis Law School, Hyderabad

Abstract

As the world aged, it encompassed with it all the things to make everyday life easier. The technology advanced and brought with it the one thing nobody can survive without today- Internet. The accessibility increased, the world was on the fingertips of anyone and everybody within seconds. But such a booming advancement didn't come without its drawbacks as it made its users susceptible to vulnerability. However, even this thriving technology couldn't be used efficiently to tame the abuse caused by the billions of people hiding behind the screen.

Cyber crime has been skyrocketing each day and even though the protectors of law have been punishing the abusers, there's a need to prevent the abuse before it happens. Cyber voyeurism, the crime of placing forth private acts of individuals without consent before the eyes of the entire world. Cyber crimes are committed by unnamed and faceless criminals, making it the most threatening crime and creating a hostile environment for all the unsuspecting targets.

The gaps which are predominant in the legal system must be filled. The research demonstrates ways to broaden the interpretation of legislatures to thwart cyber crimes. A legal framework to enable security of those individuals is required. The faceless must be named to give life to accountability of persons on internet. Persons hiding behind the screens are aware they can get away with a lot of acts and this convenience shouldn't persist.

Key Words: Cyber crime, Cyber security, Privacy, voyeurism, India, law

Cyber Insurance: A Guard Against Cyber Attacks

Deepica Gautam, Reseach Scholar, HPU, Shimla

Abstract

With the advancement of internet, digitalisation have touched upon all entities whether individuals, corporate or government. Digitalisation means anything and everything in e-format. Tonnes of data is generated which becomes an asset to the government or corporations. The corporations use this digital data to increase their business. However, if there is any unauthorised access or breach, such as identity theft, hacking, network lockdowns, cyber terrorism to name a few, then it is known as cyber crime.

In order to protect digital data, Cyber Laws are enacted which are punitive in nature. The Information Technology Act, 2000 provides for punishment to the person who tampers

with the digital data. However, that is not sufficient to an entity because the financial implications of the cyber attack have a huge impact on any organisation's balance sheet. Hence, to keep the business running smoothly, it is imperative that a solution exist, which may not be able to protect the organisation from a cyber attack, but can keep business on stable financial footing when a significant breach occurs. This paper offers a solution in the form of cyber insurance coverage. Cyber insurance has its roots in 'errors and omissions' policy and is designed to guard business from potential effects of cyber attacks so as to mitigate cyber losses.

This paper enables to understand the concept of cyber insurance and the need to extend such insurance coverage to all corporate entities as well as engage in making insurance coverage to start-ups.

Key Words: cyber crime, cyber insurance, cyber attacks, Information Technology Act.

Legal Challenges Before Cyber Law

Abhijit Das Sr O.S (Estate Court) (Town Service – Town Administration) Steel Authority of India Limited (SAIL / Durgapur Steel Plant) Durgapur

Abstract

The Cyber Laws within the Information Technology Act ,2000 and its Amendment(s) falling as Residuary subject empowered under the Parliament faces a constant hazardous position of legal control due to the uprising trends, moreover aided with Digital Technology including : Spam Laws, Laws governing Cloud Computing , Mobile Laws , Cyber Security concerning legal issues , Social Media and its legal problems .

The emergence of ITA, 2000 not only gave legal recognition to the Digital Signature and the Electronic Documents concerning Authentication of Valid Contracts , but also imposed civil liability via civil compensation to the victims u/s 43 Chapter XI of ITA,2000 superseding the governance of CPC was ensured to approximation within 4-6 Months by enabling later on the formation of two judicial authorities-(i) Cyber Appellate Tribunal in 2007 (ii) Adjudicating Officer in 2003. Indian Government was pressurized to review ITA, 2000 when CEO was charged by invoking Section 67, ITA, 2000 read with Section 85 in bazee.com case, 2004. Information Security under ITA Amendment Act, 2008 effectiveness was notified under the active alertness of Mumbai Government with by a set of Rules governing Sections -69, 69A, 69B and 70A . Further, in April, 2011, draft notifications u/s (s)- 43A and 79 and draft regulation for Cyber Cafes and u/s 6A draft regulation for E Governance delivery was released . Section 79 though defines "due diligence" under the notification defined by MCIT but in reality it is misused in the sense of Internet Censorship.

Data Theft: A Modern-Day Burglary

Dharamender Singh and Bhawani Thakur- UILS, Chandigarh University ,Punjab

Abstract

In the modern era of technology, where every other individual is having a personal gadget, although the word personal does not limit the device by simply having a fingerprint unlock or the pin-password or a pattern password, according to a survey by eMarketer in 2015, India is estimated to have over 800 million mobile phone users in 2019.Internet have every information of seconds about every individual in the world, who we meet, where we go, where we live, what kind of activities we are performing, our likes and dislikes, etc. and the

list goes on and on. Every data scientists in the world have a common phrase and is also acceptable in this technologically civilized society, that the "Internet knows better than we know ourselves". Though yet the common individual is not targeted directly but the user is indirectly a customer in the internet, big data companies does not have any specific law to protect our information, and without thinking a bit sells to the other commerce site which then will show the targeted ads to the user of internet, user do work and the ads will follow everywhere. This was one example, of data selling, and there are many more in the paper. Although this information is of high level coded language which is not easily cracked by the individuals, it is saved in the binary language or any coded language. Will the Data Localization can help secure our information? Is it sufficient? Till what extent it is secure? We have enough physical laws for crime to pay, why not sufficient numbers of laws on data, where the individuals' information is privacy based information? Even the end to end encryptions feature of social network conversation between two or more can be read, and the forwarded massage trail can be found out. This paper is divided into 5 parts, the 1st part will be dealing with the in-depth knowledge of data i.e. the introduction to this paper, 2nd part discusses the crime that can be committed by data and some of the famous criminal cases done on the basis of this data, 3rd part of the paper is a basic question: "Is your data secure?", 4th part of the laws in India and the world protecting data in cyberspace, Last and the 5th part of the paper is the conclusion and the solution that can be implemented to protect individuals data.

Cyber Stalking: Another Form Of Sexual Harassment

Shrvan Kumar Lahoti,
Student, Himachal Pradesh National Law University Shimla

Abstract

"Cyber stalking refers to use of technology i.e. internet, e-mail, or other telecommunication technologies to harass or stalk another person. It is not the mere annoyance of unsolicited e-mail rather a methodical, deliberate, and persistent. It is an extension of the physical form of stalking. A cyberstalker only needs access to a computer or modem, and can easily locate private information about a potential victim within a few mouse clicks or key strokes. This paper addresses and analyses growing threat of sexual harassment in cyberspace. Over the years, digital transactions and communications have been increasingly transpiring at an accelerated rate. Sexual harassment is considered to be a major threat and obstacle to the free, legitimate, functional and joyful use of the Net. Online sexual harassment has become a serious and social concern. Solution is not necessarily to avoid the internet and other digital technologies; rather, more internet safety education and prevention information are needed to raise awareness among youth, adults and practitioners.

"Cyber Voyeurism Against Woman In India"

Nikita Bokil & Grishma Mahatme,
Student, Symbiosis Law School, Pune

ABSTRACT

The crime rate against women is on an increasing pace in India. Not only physically but also on a digital platform the safety of a woman is deeply questioned in today's scenario. Cyber Voyeurism is one of those digital crime which is creating its path to the destruction of digital

and technological safety of an individual. Cyber Voyeurism though not being gender specific is experienced on a large scale by the women in this world. One of the most important right acquired by any citizen, is the right to privacy and endangering this right though would not cause any physical harm but the damage done to the mental state and stability of a person cannot be substituted, hence the crime of voyeurism should be treated at par to the other crimes against body of a person. Through this paper, a comparative detailed study of the crime of voyeurism in the digital space against women will be dealt with. The paper will also comprise of the evolution of the concept of cyber voyeurism in India. Since the world is progressing towards embracing the technology and innovations offered, the negatives emerging with it are often been neglected. Therefore, the scenario regarding digital voyeurism in various countries is also discussed and a comparative analysis is made with respect to India. The main purpose of the paper is to give light to the provisions available in India against the crime of cyber voyeurism and what changes are required to make the law more stringent.

Cyber Voyeurism: Your Privacy Has Been Hacked

Akanksha Sahoo and Harleen Kaur Rait, BBA.LLB student,
Symbosis Law School, Hyderabad

Abstract

"The cyber world is sort of wild and to some degree we are asked to be the sheriff."

Internet emerged as a bright light which shone over the world to perpetuate an array of advancements in technology. With each passing day the electronic technology grows by leaps and bounds which places the whole world at the fingertips of a person, within seconds. As every coin has two sides, technology did not come without its drawbacks. Electronic harassment emerges as a threatening behaviour in the cyber world. Cyber voyeurism has been booming in the society as a Paraphilic disorder which is spreading as a virus within India as well. One single vulnerability is all an attacker needs. There is no limit to the abundance of content on internet and the onus to prevent its misuse lies on us as well as the government. Now, the internet has taken virtual voyeurism to new heights.

The thing about laws relating to voyeurism is that there is insufficient material available in print at present. The research revolves around underlining the aspects and filing the gaps in the present legal system with respect to the cyber laws. The research is not limited to defining voyeurism but expands towards the reason behind the commission of this crime. It indulges in enabling blockage of such content which breaches privacy in order to make internet a secure space.

Keywords: Cyber voyeurism, electronic harassment, Cyber stalking, Cyber security, Privacy, India, Law

Cyber Stalking – Law And Safety In India

Daizy Thakur, PhD Research Scholar Himachal Pradesh University

Abstract

Technology is now a necessity of today's world. Its growth in last few years has been immense. Technology is a double-edged sword as it has brought in so many good changes but you also cannot ignore the rise of cybercrimes which are at an all time high. As technology became more easily available to the people cybercrimes have evolved profoundly. One such

crime is cyberstalking. Cyberstalking is often termed as an obsessive behaviour in which a person compulsively and illegally keeps a track of someone's each and every activity over the internet. Cyberstalking can cause extreme distress for the victim. It can impact their career, personal relationships, and quality of life. Cyberstalking is an escalated form of online harassment directed at a specific person that causes emotional suffering with no legitimate purpose. The action is to annoy, alarm, and emotionally abuse another person. Anonymity, easy avail & low cost make the internet safe heavens for cyber stalkers. It has become imperative to make strong laws to address such cyber threats. India is also working on to address these threats with strong legal framework but has a long way to go. Technology is a boon but it can turn into a curse easily, so utmost care and preventive measures should be taken while using it.

Data Leakage In Cyber Security

Ahanksha Singh, ,Bishi Sharma Students,
BBA.LLB 3 Rd Year ,Banasthali Vidyapith, Jaipur, Rajasthan

Abstract

Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically. Data leakage threats usually occur via the web and email, but can also occur via mobile data storage devices such as optical media, USB keys, and laptops.Barely a day goes by without a confidential data breach hitting the headlines. Data leakage, also known as low and slow data theft, is a huge problem for data security, and the damage caused to any organization, regardless of size or industry, can be serious.There are many different types of data leakage and it is important to understand that the problem can be initiated via external or internal source. Protective measures need to address all areas to ensure that the most common data leakage threats are prevented. "Unauthorized" data leakage does not necessarily mean intended or malicious. The good news is that the majority of data leakage incidents are accidental. For example, an employee may unintentionally choose the wrong recipient when sending an email containing confidential data. Unfortunately, unintentional data leakage can still result in the same penalties and reputational damage as they do not mitigate legal responsibilities. The threat is real, and real threats need serious data leakage prevention.

Data Privacy And Its Legal Protection In India: A Critique

Ankit Raj Rajial, Ph.D. Research Scholar, HPU, Deptt. of Laws

Abstract

The digital revolution has changed the methods of information sharing throughout the world. The development of internet and its penetration into the lives of people has made the life easier. Further, with the increasing penetration of mobile phones internet has become an indispensable thing for the modern life. People while using these devices connected through internet are leaving their digital footprints in the form of user data. The Internet of Things (IoT) has further accentuated the generation of data in large quantities. The browsing data of an individual is his own created and has his privacy implications associated with it. After the supreme court of India bringing the privacy at the altar of constitutional protection, the data privacy has assumed more significance in current scenario. This data generated online has

come to be referred as the new oil of the twenty first century. Considering the value of this new oil, the countries worldwide have begun to provide for legal regulations to tap this new resource. However, the Indian law on the data protection is bit slow to respond than the rest of the world. This paper discusses the Indian law on the data privacy.

Crime Against Women Under Cyber Law

Bhumika Bhargava, Shivangi Tiwari,
Institute Of Law Jiwaji University Gwalior

Abstract

Let us consider cases where so-called conventional crimes are carried out using computer or the Inherent as a tool. Consider cases of spread of phonographic material, Criminal threats delivered via email, website that defame someone or spread racial hatred etc. In all these cases, the computer is merely incidental to the crime. Distributing pamphlets promoting racial enmity is in essence similar to putting up a website promoting such I'll feelings. In 2013, according to the Internet World Stats Report, 137,000,000 people used Internet, and 56,698,300 people used Face book in India, as a result there arises a concern for Internet safety. The increased use of the Internet has created an impact on the number of online cyber crime. .In 2001 India's first cyber stalking case was reported. Manish Kathuria was stalking an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, www.mirc.com using her name; and used obscene and obnoxious language, and distributed her residence telephone number, invited people to chat with her on the phone. As a result, Ms. Ritu Kohli was getting obscene calls from various states of India and abroad, and people were talking dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Kohli. But Section 509 refers only to a word, a gesture or an act intended to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section. This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding protection of victim.

Social Media And Religious Hate Speech In India

R. Dinesh Kumar, B.A, Ll. B (Hons).,
Vels School Of Law, Chennai.

Abstract

Social media became an inevitable element of our regular life. Allowing us to connect from various parts of the society, to share valuable information and ideas to other people at a very large stake. Indian society witnessed a skyrocketing growth in social media usage, with large internet infrastructure India's social media usage reached up to 326 million users in the year of 2018. However, in recent times social media became propaganda platform to spread hate speech in India. People with hidden political and ideological agendas spreading hatred towards people of other religions and communities. This catastrophic usage of social media slowly becoming a casual trend in India, often leads to victimization of innocent people of other community. This paper aims to analyze pattern of increasing religious hate speech in India, to study laws relating to curb hate speech in India and obligation of social media to eliminate hate speech in their online social platform.

KEYWORDS: skyrocketing, catastrophic, victimization, community, social-platform agendas

Cyber Crimes – Ways To Curb.

Rahimunnisa Begum, Faculty Of Law,
Gitam Deemed To Be University

Abstract

India, at the global front is known for its values, ethics, morals and Agro-based produce apart from playing a major role in terms of contributing as the best in the World Human IT Professionals supplier. This identity has its stake in IT related sector's as well. We the Indian's play very significant role in the field of Information Technology. Our services are applauded right from the 'key board operator' to the range of CEO s in the Information Technology sector. We are equally good in numbers in the IT dominated core fields such as, Technocrats, Software professionals, and allied fields of Tele communications, Embedded systems, Web design, Satellite Channels etc.

This adds lot of glory to the Crown of Democratic India. Equally, it's not at all surprise that we stand "neck to neck" in Commission as well as targets of "Cyber Crime's". We stand tall today in the global arena as 'victim's of Technology". This menace no doubt is "Global", but the repercussions are uncompromisingly high on the local areas too. The worst ever victims are 'We the Indian's'....greater extent are innocent non-tech savvy citizen's.

The crimes against the property, individual, state, organisation and the state at large are the categories of Cyber crimes which includes phishing, bank frauds, mobile frauds, data piracy, infringement of Intellectual property rights etc. to name a few of the big list of cyber crimes. Need of the hour is to trace out legal and technological safeguards.

Let us all stand united to fight against this 'Societal crime' and prove our unity once again in combating "Cyber Crimes"

Emerging Challenges Before Cyber Law

Dharvi & Himanshu , students of BA.LL.B 4th year
JIMS school of Law, GGS IP University

Abstract

The rapid growth in the field of information and communication technology has given rise to cyber world constituting cyber space. In today's world we are highly connected or linked up by various social media application to have conversation or to fetch any guidance or information or to make any transaction etc. and the number of internet users are increasing tremendously every year and at the same time there is increase in number of people using smart phones. So, securing the information of the user have become the major concern and biggest challenge.

Whenever we talk about cyber world or digitalization what comes first in our mind is that Safe, Is This Secure? ***In Bazee.com Case 2008***: In December 2004 the chief executive officer of Bazee.com was arrested because he was selling a compact disk (CD) with offensive material on the website, and even CD was also sold conjointly sold out in the market of Delhi. The Delhi Police and therefore the Mumbai Police got into action and later the CEO free on bail.

People are connecting with world wide web like never before making a way to digital revolution. To fight against cyber crime we need a comprehensive and safer approach mere

giving of some preventive measures alone cannot prevent cyber crime, we need a proper law and enforcement for this. The cyber law in India is inexistence with Indian Penal Code, 1860, IT Act, 2000 and ITA-2000 (Amendment) in its place further it still has lot of issues and challenges. This paper's major concern is the challenges faced by cyber world in context to security and privacy of the users who access various applications and websites as today day by day we are moving towards more digitalization and being paper less movement. This paper also focuses on the cyber security, cyber security techniques, and trends changing cyber security.

Cyber Crimes Against Woman In India And The Law

Rupesh Kumar, Researcher, Punjabi University

Abstract

The whole World stepped towards digitalization which automatically brought technological power. People explore using internet and made more life comfortable and easy. They explore the unknown people through internet and communicate with anyone, anytime, anywhere across the Global. The digital space has opened and widened doors to cyber crimes and mostly woman is their target than man. Nowadays cyber-crime has emerged as a mainand important challenge for law enforcement agencies in the India. In technological era women and children always remain at high risk. Offenders are gradually misusing cyber platforms to abuse and harass children and women for voyeuristic pleasures in our Country. A modernization of the conventional set up, preventiveand equipped police personnel and cyber crime control agency with utmost skills and knowledge is for control and prevention of cyber-crime. This paper throws light on numerous cybercrimes and various legislative measures to tackle them. A model is proposed and specify preventative numerous initiatives specifically to eradicate cyber-crime against children and woman.

Keywords- Cyber Crime, Cyber Harassment, Cyber Stalking, Woman Empowerment, Cyber Law

Cyber World: A Whisper Network Of Harrassments?

Siddharth Kumar & Aniket Singh, B.A. LL.B (Hons.) 2nd Year Student At H.P. National Law University, Shimla.

Abstract

"Rather than shaming the woman for having her pictures splashed over revenge porn websites, people should extend their support and shame the criminal instead."

— Anangsha Alammyan

As the Internet becomes a significant part of human existence and a critical space for the voice of marginalized population to be acknowledged, a woman's inability to feel safe online is an impediment to her freedom and to her basic human rights. Yet the issue of online violence and harassment is often overlooked in discussions of violence against women. The problem is highly

under-reported. The severity of violence is likely to be under-emphasized because the correlation

between injuries sustained as a result of violence varies very little between severe and less severeinstances of barbarity. It is a clear expression of gender discrimination and inequality

that exists offline. Online, it simply amplifies. The first step to addressing online violence against women is to recognize that it is a legitimate and harmful manifestation of gender-based violence. In India, like anywhere else, online violence and harassment of women and marginalized genders and sexualities is rampant, in contrast to Internet's initial premise of equal opportunity and neutrality. The epidemic of bullying has been another attention seeking problem in the internet. This can take the form of hacking, morphing of photographs, fake profiles on social networking sites or circulation of images without their consent – not from strangers alone but from those known to them. Or it can take the form of gendered hate mail, sexualized slurs, and uncomfortable references to body, nudity, sex life, and rape threats, which sometimes turn out to be explicit and graphic. Finally the authors will present a book review on a controversial book I Am a Troll: Inside the Secret World of the BJP's Digital Army which will help the readers to break the preconceived notions regarding the Cyber World and Cyber Crime.

KEYWORDS: - Cyber world, online, harassment, women, crime, social network.

Information Warfare: A New Face Of Terrrorism?

Veena Chandra (Hidayatullah National Law University,Raipur(C.G))

Abstract

The growing importance of information and communication infrastructure has opened up unprecedented perils of terrorism. Hence, it becomes necessary to distinguish between the bulk of Cyber warfare literature which addresses the military dimension and information warfare which has expanded into non-military dimension. Literature of cyber warfare deals with attacks on system which might include complete system shutdown. However, it does not restrict to only system shutdown but also consists attacks on power grids, or aircraft avionic systems. Typically, they are intended to cause chaos. In Information warfare, the weapon of destruction is the Information or data itself which typically gives a party an unfair advantage over the others in the battlefield by disrupting the data or the Information, the target is to mainlyto cause harm to the public services. The objective of this paper is to trace out how the Information Warfare has bigger face of terrorism by entering the public domain due to lower entry barriers for cyber attackers and increased economic dependency on information infrastructure. Corporate espionage and perception management are few things that make the problem of Information Warfare a larger issue with an urgent necessity of discussion. This paper shall discuss above mentioned key issues along with ancillary lines of arguments using various conventions and judicial precedents with global perspective.

Reason Of Women's Vulnerability: Cybercrimes

Devansh Solanki & Jannat Garg, LLOYD LAW COLLEGE

Abstract

Crimes against women form a crucial part of cybercrimes in India and the online platform is now the new platform where women's dignity, privacy and security are increasingly being challenged every moment. The paper argues the question is how the diverse concerns of the government match up with the specialized security needs of their female citizens, who are the most vulnerable one. The paper will briefly examine various National laws like section 67(a),

67(b) and 72 of the Information Technology Act 2000. The 2013 Criminal Amendment Act to the Indian Penal Code, 1860 by way of Section 354A to Section 354D, Indecent Representation of Women (Prohibition) Bill, 2012. The paper will be taking assistance of various reputed cases like Ritu Kohli case, Delhi Metro CCTV Footage Leak case, DPS MMS Scandal, Bal Bharti Case etc. in cybercrime to arrive at our conclusion. The questionnaire typically consisted 9 questions which are a mix of close-ended questions and open-ended questions. It is observed that a huge number of population considers the women as disadvantaged group and considers Internet as basic platform for occurring of various crimes against women. Also, most of the respondents does not considers the national laws as sufficient for women due to lack of proper implementation in the country and also lack of government based mechanisms. Most of the population opted for Facebook as the highest crime occurring site. It also includes conclusion and some suggestions to curb the cyber-crime against women.

Keywords: cybercrime, India, women, crime against women

Cyber Voyeurism ; An End To Privacy

Janvi Goyal, Himachal Pradesh National Law University

Abstract

Women, since time immemorial have remained victims of various forms of sexual offences. With the recent advancements in the field of science and technology, they have become victims of a Cyber voyeurism, an emerging sex crime which has taken the internet by storm.voyeurism--“to peep somebody” has been part of human history since our inception. But television and now the Internet seem only to have whetted our natural voyeuristic special laws to protect women in this sphere, and prohibits a man from watching or capturing the image of a woman engaging in a private act. In most cases, the voyeur does not have to make direct interaction with the subject of his interest, and hence they are often unaware of the fact that they are being observed. This in-turn reduces the possibility of such offences being reported, which leaves the victims in a situation where they are subjected to grave injustice and violation of human dignity, although they may not be aware of the same. This paper attempts to study the lacunae in the implementation of legislations relating to cyber voyeurism in India and suggest for procedures to be adopted by the legislature so as to effectively combat voyeurism and similar sex crimes that have crept into the cyber world.The purpose of this issue paper is to lay out the key legal, institutional and ethical issues concerning technology-mediated Violence against Women (VAW), to raise critical questions for further deliberation and action.

Jurisdiction In Cyber Law

Shubham Sharma, BA LLB 2nd Year ,
Delhi Metropolitan Education

Abstract

Since the inception of cyberspace, e-commerce and exchange of digital information have induced a shift in the traditional ways of business. In the 21st century, the internet hosts the majority of commercial activities around the globe. The architecture of the internet is

transnational and limitless. The lack of any formal borders results in easy access with minimum restrictions. This facilitates convulsive issues going beyond regional or even national boundaries. Such disputes come under the ambit of Cyber Law. The local jurisdiction laws of a state often fail to suffice on account of the borderless extent of the internet. In case of disputes arising out of trade of tangible goods, law enforcement is a smooth process. But in case of Intellectual Property Rights (hereinafter, IPR), being infringed in a foreign land can make the identification of jurisdiction a difficult task. Courts of many countries have propounded various tests and rules to identify the extent of their jurisdiction. The article aims to enlist and analyse these methods. It explores the underlying problems that arise due to the un-harmonised laws of different countries and organisations. It also discusses at length, the IPR issues that arise in different countries including India.

Child Pornography, Effectiveness Of Laws In India

Meenu, Assistant Professor, H.P College Of Law, Kala-Amb

Abstract

Children are the wealth of nation. They are creators and shapers of country. Today's child became the adult for tomorrow. If our today is secure then our tomorrow automatically safe. Day to day increasing crime in cyber space badly affects our child also. In recent years pornography has established as a big industry at international level. Child pornography is more dangerous rather than adult pornography, because child is immature and unable to understand right and wrong. Child pornography is considered as an offence in Indian society. It is sexual exploitation of a child. Federal law defines child pornography as visual depiction of sexually explicit conduct involving minor. 25 million images are reviewed by the national center for missing and exploited children annually. That is 480,769 images per week. One out of three girls and one out of five boys will be sexually abused before they reach 18 years. In order to control the heinous crime of sexual abuse and sexual exploitation of children the ministry of women and child development introduced the POSCO Act 2012. This paper is aggressive attempt to understand the various sections of POCSO Act and 66A which is regarding the punishment for those persons who has involved to exploit the children who has not attained the age of 18 years. This study is also remarks the various judgments given by different courts. It is also an attempt to understand how this industry eludes the Police and how to make them accountable for their crime through stringent laws.

Online Frauds: Challenges And Strive To Prevent E-Frauds

Mohammad Irfan & Devansh Agarwal, School Of Law, Galgotias University

Abstract

"Every once in a while, a new technology, an old problem and a big idea turns into an innovation" *Dean Kamen*

As we are observing from the past few decades that there has been a tremendous revolution in computing and communication and use of this information technology is increasing in a rapid way. Every now and then, new faster and better technologies are emerging in the market. In the olden days, there were no such awareness about these kinds of technologies but as time passed, the society started taking more and more interest in these technologies as they were

cheaper and reliable. Moreover, after the emergence of E-commerce, the pace of growth of technology increased even faster and the people started indulging more into it. Secondly, the era of Digital Banking System, where a person can transfer the huge amount of money within minutes from one account to other in addition to which the most important thing to be covered is the various platform of online jobs where people are making money sitting back at homes in front of their computer screens rather than doing hectic field jobs which are even tough to get. The concept of digital banking system where banks claim that their systems are fool proof, still nowadays we often hear about online frauds and forgery for crores of rupees.
Last but not the least, our privacy has been compromised by different social media cites including issues like leaking of private photos and Confidential information or getting other information by making fake ID's. 'Phishing' the most unethical and fraudulent way of getting someone's personal information with the intention to blackmail that person by just giving him an unauthorised pop up and to hack his computer. Lastly we can say that many Laws have been made to control all this irrelevant things but still there are no such proper departments allotted which can handle all this abrupt activities due to which the Criminals take more and more advantage and it gives them immense courage to indulge more into it as there is no tight securities as such.

The Holistic Cyber Security In National Defence And Its Dimensions

C. Naveen Kumar, School Of Excellence In Law, Chennai

Abstract

"DIGITAL INDIA- POWER TO EMPOWER" we are in the era of digital India movement. The government of India emphasis to foster a digitally empowered society in all manners. According to Mary Meeker 2019 Report, India has the second-largest Internet user-base ranking at 12 per cent. Consequently, The Indian cyber defence is rated low as compared to the international frameworks. This paper expostulates about the policy like National Cyber Security Policy, 2013 and cyber security agencies and teams, which advocates cyber security in India. It is also segregated into civilian cyber security and military cyber security. Every exertion in Cyberspace will have a cyber legal standpoint by implementing the Information Technology Act, 2000 in India. There are also various complications for implementing the cyber security in India due to digital illiteracy, low Internet speed, lack of qualified persons in cyber technology, and lack of knowledge about the jeopardy of cyberspace. Hence, an attempt has been made in this paper to perceive that the cyber defence is an important national defence for national security and it also addresses their challenges with some medication. This paper also highlights the international cyber security, cyber-attacks, legal frameworks and policies, which are taken to govern the cybercrimes.

The Plight Of Digital Data Protection In The Age Of Communication And Technology: A Study Of Indian Legislative

Nidhi Sharma, Assistant Professor,
School of Law Manipal University Jaipur

Abstract

In today's era, there has been blistering development in communication and technology. While interacting in daily life, technology is becoming indispensable for each owing to its

round the clock proximity, convenience, and immediacy. The pace at which an individual's life is becoming intrinsically intertwined with technology, speaks volumes about the threats it poses to one's privacy. A user while browsing online is often dangerously oblivious to the number of digital footprints he leaves behind. Either the users are not cautious or are unaware while surfing online about the threats and challenges that technology poses and the outdated legal mechanisms add misery to the cause. This study will examine the legal regime for securing the right to digital privacy in India. In doing so, the efficacy of existing legal provisions and the Personal Data Protection Bill, 2019 will be assessed on the touchstone of the EU General Data Protection Regulation (GDPR). In the new era of informational technology, this paper calls for the strengthening of the legal mechanism to protect data with sufficient safeguards to incorporate flexible measures to address the unprecedented development of technology.

Keywords: Technology, digital privacy, digital footprints, data protection laws, GDPR.

Privacy & Data Protection In Cyber Space

Nikhil Sanadhaya & Ayush Kumar, Jaipur National University

Abstract

With the advancement in technology and emergence of internet and then various social interaction platforms such as facebook, instagram, snapchat, etc. the issue of privacy was initial not taken into concern but now it has become a major issue. In recent times there was news that European Union has fined Google with billions of dollars for the privacy breach. Last year a controversy related to Cambridge analytica and popular social media platform facebook grabed huge attention and facebook received huge criticism after this controversy. In cyberspace the issue related to privacy and data protection has became a major concern for legal intellectuals all over the globe.. Globalization has given acceptance of technology in the whole world, as per growing requirement different countries has introduced different legal framework like DPA (Data Protection Act)1998 UK, ECPA(Electronic Communications Privacy Act of 1986)USA etc. from time to time, but in India there is no such comprehensive legal framework that deals with privacy issue. To handle major cyber challenges we refer ITA Act 2008 that was built with the motivation to facilitate e-commerce and hence the privacy was not prior concern in IT act. This suggestive framework provides comprehensive solution as per present and future requirements of privacy. As rightly said "true power of any law lies on its ability and ease of enforcement".

"Emerging Trends In Cyber World And Law"

Dr. (Mrs.) Seema Kashyap & Anirudh Sood,
Assistant Professor In Law At Himachal Pradesh University Institute Of Legal Studies

Abstract

Statistically true, Indian demographics includes a considerable number of netizens majority of which is in the tender age group of 10-18 years. There is no gainsaying that thus far, cheap high speed data plans alone accounts for ever increasing number of smartphone users as also users with internet accessibility at ease. Everything seems to be a click away. What is even concerning is the easy availability of unfiltered and unregulated content on the social media platforms, the active supporters of such platforms may vehemently argue that

these were devised to share posts, thoughts, photos and other multimedia. Our concern as also perception stands corroborated by a recent incident relating to Tiktok, an online video sharing app, which suffered the wrath of Hon'ble Madras High Court on the premise that it encourages pornography. Though later on the earlier position got restituted. This is exactly where the freedom of expression comes in conflict with public decency and morality. What appears to be important for consideration is that whether every notorious and enticing act, though not seditious, can be allowed to be publicly exhibited even if the same is capable of corrupting the young innocent minds. It is in this backdrop that the need for regulation of online content has arisen. Unregulated, unchecked and non restrictive proliferation of the content can have devastating effect. This we say so keeping in view there percussions of an online game by the name of Blue Whale which the nation has witnessed in the past couple of months. To our dismay, no efficacious policy dealing with the issue in hand has been envisaged. This research paper is an attempt to highlight the emerging trends in the cyber world and the mechanisms, existing as well as needed, for dealing with the challenges accompanying the emerging dimensions of cyber world in the present time.

Online Banking Frauds In India: Legal Protection In Cyber World

Dinesh Dayma, Assistant Professor Of Law,
Faculty Of Law, University Of Delhi.

Abstract

Certainly the use of technology in the financial services sector for their development has been a tremendous encouragement. However, business and payment transactions to be carried out due to heavy reliance on electronic and digital equipment, a serious threat to the safety and reliability of financial operations are imposed. With the growing trend of online and cyber transactions, banking scandals, the number of banking technology tool use is increasing more and more people are affected. Online Banking frauds are separate category of criminal offences under various legal provisions in India. These offences not only victimize individuals with pecuniary loss but can also have serious repercussions on the national economy. Online banking frauds-such as data theft, forgery, online fraud, data privacy, etc. are crimes which evoke serious concern and impact on the Nation’s security and governance. This paper seeks to present a perspective on the trend of crimes and legislative measures to deal with such crimes in India.

AADHAR- A SUMPTUOUS TREAT FOR CYBER CRIMINALS

R. Rebecca Vasanthini Percy (School Of Excellence in Law, Chennai)

Abstract

This paper focuses on the evolution, data protection, privacy policies and smack of Aadhar on India’s national digital biometric identity system. An identity scheme is seen as a tool to avert identity fraud and enabling social inclusion to be the paramount hub of a national identity scheme, for this purpose the contemporary design of the Aadhar is implemented but it is lured to criticisms. The protection of data is a major challenge for the UIDAI. Any attack on UIDAI data can immobilize Indian businesses and administration which results in a huge privation to the country’s economy and the seclusion of its citizens. There are various outrageous incidents where the privacy of the citizens was breached by Aadhar. Three lakhs

of Aadhar data got lost with PAN in Maharastra. In Kerala, Aadhar data of over thirty five lakhs of pensioner has been leaked from the Kerala State Pension Department. As the major concern for security and privacy data, UIDAI moved Heaven and Earth and adopted a new encryption standard on the Aadhar biometric device and only registered devices were allowed to make Aadhar transactions but usage of biometric leads to security threats. The illustrious dream of digital India could simply be a holocaust if a billion countrymen eventually get digitalised and a single hack gives malevolent hackers a lifespan access to their digital assets and congruence. Thus Aadhar is "A Blessing in Disguise" but it is a "Bite of more than we can Chew"

Cyber Attack: Modern Day Weaponry

Rajat & Shrishti Mishra(Chandigarh University)

Abstract

Now we are living in an era of cyber warfare. In this research paper we'll talk about cyber attacks which are conducted by governmental agency. Like, USA's cyber attack on Iran Revolutionary guard was the revert back by the side of USA where Theran says no cyber attack on Iran by enemies has been successful, as the USA said of launching cyber attack, targeting Iranian military. Well if we look in the history then we'll find that this is not the first time when USA implements cyber attack on any country. USA and Iran previously engaged in cyber warfare. Nine year back USA and Israel started an operation "Operation Olympic Games". At that time USA and Israel used the so called Stuxnet virus to disrupt centrifuges at an Iranian uranium enrichment facility. In 2012 Iran showed its capabilities when it infected Saudi state-owned oil company Saudi Aramco with a virus that erased data on 30,000 computers. Now all superpower countries are investing huge amount of money in their cyber agency. Here the question is what India needs to learn for the time being regarding cyber attack. And what would be the chances of being cyber attacked by other military agency and our future plan for being offensive and defensive in nature and how this will affect future war. This research paper highlights the impact of such attacks, its range and countermeasure to prevent it.

Crime Against Children In Cyber World (Child Pornography, Sextortion, Indecent Representation)

Parusha Shridhar & Kumari Babita, Chandigarh University

Abstract

This paper is attempted to access the connotation of cybercrimes within the ambit of cybercrimes against children and have attempted to understand the heinousness of such offences and their multiplying rate over the ages in lieu of advancing technology and flourishing ease of access to digital content. Bodily satisfaction is the uttermost natural human need to exist and hence, sexual crimes have always existed in one form of the other. The purpose of this paper is to shed light on the sexual crimes against children in the cyber world and the real world repercussions of the same. The paper focuses majorly on offences of (I) Child Pornography, (II) Sextortion and (III) Indecent Representation. Cyber space is a new growing arena that is serving as a medium for the old offences and is aiding their unchecked, rapid and grave impact on children and society at large. Since, cybercrime has

emerged as the newest and possibly most labyrinthine criminal agency; its challenges are equally different and grave. The paper aims at the issues, namely, (I) Ease of access to children,(II)Jurisdiction and (III) Vague Laws. The amendments made in POSCO Act,2012, IT Act,2000, with respect to child pornography, coupled with important precedents of KamleshVaswani V. Union of India &Ors and The Tiktok Chinese Application ban order have been analyzed to understand the recent developments in judicial forum to curb the exploitation and victimization of children. Child pornography not only has indecent exposure to children but has psychological impacts too.

Cyberspace-An Era Of Refining Human Civilization Or Draconian To Sovereignty Of Civilised Society

Pranav Kumar Kaushal & Priyamvada Kaushal,
Student B.A.L.L.B, Bahra University Shimla

Abstract

The era of World Wide Web and modern computer technologies has entered into the lives of each and every individual just like the oxygen to a normal human being. As human beings cannot survive without oxygen similarly human beings in the 21st century cannot survive without these modern computer technologies. The ability of the World Wide Web to penetrate in every home and community across the globe has both positive and negative implications. On one hand these modern technologies have been considered as invaluable storehouse of information, research and discovery while on the other hand, these modern technologies can be seen to override and destroy community morals, values and standards subjecting to challenge the sovereignty of the civilised society. This article deals with the landscape of cyber crimes, cyber space, economic crime and technologies as means of information society.

Keywords:- Child Pornography, Jurisdiction, POSCO ACT, Porn Ban, Psychological impact

Privacy, Defamation & Data Protection In Cyber Space

Devanshi Goyal & Surbhi Jain (B com..LLB.(HONS) 4th YEAR,
Jagran Lakecity University, School of Law, Bhopal)

Abstract

“Privatus is the latin word which means separate from all around ”. Privacy is the right of everyone that every person should get their place to resist and peace, or freedom from interference by anybody in their personal data. Privacy can be of individual or a group which need to secluded from other peoples or there can be a private data that need to be protected. It is the natural right because every person has their specific comfort area where they can keep their information to the limited area. Cyberspace is interconnected technology, it is fully electronic world created by networks in parallel with our environment. It is the global computer network to facilitate online communication. It is the medium through which users are allowed to share information, interact, swap ideas, play games, conduct business connectivity globally and many other activities. It is a medium for social interaction, rather than its technical execution and implementation. Data protection act lays down that you must have a legitimate reason for processing a personal information and the individual who's

information is being processed out has must given a explicit consent for it. Consent is the basis for the data protection as it gives the authorization to handle ones personal information however consent is not defined in data protection act but it signifies the importance consent in it. Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. Privacy is an individual's choice that what to access, when to access and who can access. To safeguard the privacy of an individual as it goes hand-in-hand in cyberspace since the latter is protected and former will not be invaded. Since the internet has existed the online data is in threat by cybercriminals and hackers to the epidemic proportion. To protect individual expectation of privacy in cyberspace by the law is the biggest problem. It further explains the legal descriptions of privacy, expectation of privacy, and cyberspace. There was no definition of cyber crime earlier then it come up with IT Act, 2000 and the subsequent amendment in it, yet it is still incomplete.

Keyword: cybercriminals, consent, IT act,2000, data protection

Cyber Crimes And Their Impacts

Priyanka yadav & Ritika, B.com LLB 3rd year,
Banasthali Vidyapith, Rajasthan

Abstract

As we all know that this the era where most of the things are done usually over the internet starting from online dealing to the online transactions. Since the online is taken into account as worldwide stage, anyone can access the resources of the internet from anywhere. In the current era of on-line process, most of the knowledge is on-line and vulnerable to cyber threats. There are an enormous range of cyber threats and their behavior is troublesome to early understanding therefore troublesome to limit within the early phases of the cyber attacks. Cyber attacks could have some motivation behind it or is also processed unwittingly. The attacks those are processed wittingly can be considered as the cyber crime and they have serious impacts over the society within the kind of economical disrupt, mental disturbance, threat to National defense etc. Restriction of cyber crime depends on correct analysis of their behavior and understanding of their impacts over varied levels of society. Therefore this research paper provides the understanding of cyber crimes and their impacts over the society with the longer term trends of cyber crimes.

Data Security Concerns In Cyber Space

Ramanya Gayathri.M, Sastra Deemed to be University, Thanjavur

Abstract

Cyber space is a virtual space with no physical boundaries. It is measured as one of the technological innovations where the cyber world is ruled by netizens. Cyber space works on the basis of continous flow of information and data which contains personal and public information which need to be protected. It can be seen that issues like confidentiality and privacy of information is getting affected during the process of free flow of data. Thus various legal as well as technical regulatory mechanisms can be used to protect the data from misuse or infringement. The various threats and implications faced in safeguarding the data is enormous and only a self regulatory mechanism can provide proper shield. Even though Indian law on data protection is not in force still the provisions in the Bill can be applied in various situations. Information Technology provisions can also be affected and also the

international scenario can be taken into consideration for creating more stringent regulations for data security. As internet world is ruled by data and free flow of information, it cannot be curtailed without taking efficient means to protect the same. Free flow of data helps in growth of digital market in turn the lifeblood of global economy. It not only benefits companies in the technology and digital sectors but also those in traditional industries like banking, retail and healthcare and the growing e-commerce sector. Electronic data interchange is the mechanism by which all these fields work efficiently. Proper regulation is the only means by which these activities can be successfully performed.

Keywords - cyber space, data, information, privacy.

Recent Trends In Protecting Intellectual Property Through Cyber Laws: Indian Perspective

CS Yogesh Sharma, Assistant Professor , Maharaja Agrasen University

Abstract

Intellectual Property refers to category of law relating to the rights of the possessor of intangible products of innovation or ingenuity. Intellectual Property law awards special rights to definite owners of artistic works, technical inventions, and symbols or designs. Cyber law relatively a new field refers to the cluster of legal issues occurring with the exercise of communications technologies that create cyberspace or the Internet. These issues include intellectual property (primarily copyright and trademarks), privacy, free speech and the suitable exercise of jurisdiction and authority over transactions and communications in cyberspace. It covers criminal and civil issues ranging from financial crimes to cyber bullying to First and Fourth Amendment rights.

The introduction of Information Technology and computers in India has created a new world in the cyberspace leading to various legal challenges and at times solutions. Copyrights, trademarks, designs, layout and circuit designs in the current digital environment, are interwoven with the electronic technology therefore more affirmative protective laws are required to guard new inventions and creations and also to save the real owners from economic losses.

Therefore to understand the various legal systems that may govern this area it is essential to have knowledge of not only cyber laws and Intellectual Property Laws but also of Conflicts of Law and international law. Though diverse approaches and legislations have been enacted by the Government for delivering a secure configuration against cyber threats, however it is the duty of the owner of intellectual property right to invalidate and reduce mala fide acts of criminals by taking proactive measures. This paper explicates various issues associated with the protection of Intellectual Property through Cyber Laws in Indian.

Keywords: Cyber law, Intellectual Property, Information Technology, Computers.

Emerging Challenges Before Cyber Law

Meenakshi Gandhi, Research Scholar,
Department of Law, University of Jammu.

Abstract

ABSTRACT: The development in the Information Technology in general and the internet in particular has revolutionized the present society by enhancing the modes of communication, quality of life and has become integral part of daily life. Though with this technology

advancement we can do various works without physically going in the office, bank etc but at the same time it has made us vulnerable to the hackers who in no time can dupe us of our hard earned money. Too much dependent on cyber technology has put the government to think on the lines of security issue pertaining to the technology. With the present world shrinking into global village due to information technology (internet) the security concern by way of innovations as well as strict cyber laws is a need of an hour. Today we hear of phising, posting indecent/ pornographic material, social media crimes, worm attack, hacking of governmental sites and IPR, privacy and electronic transactions issues. The cheaper net data provided by various companies has made the people more vulnerable to cyber crimes. Thus there is a need for appropriate enabling frameworks in the shape of antivirus solutions, search engines, fool proof solutions to attack of cyber criminals and stringent laws for criminals of cyber crimes keeping in view the emerging challenges which we are facing while accessing cyber technology.

Keywords: Information Technology, security, IT-Act, ethical issues, Intellectual Property Rights.

Cyber Forensics & Electronic Evidence And Investigations

Harshita Menon ,S Vasanth. &
Rupesh Choudhary, Student, B.A.LLB, Telengana

Abstract

This paper aims to portray the various dimensions of Cyber Forensics which means application of investigation and analysis techniques in the interest of determining potential legal evidence for the purpose of collecting and preserving data and evidence for a particular criminal case, from computing devices. It is often used by law enforcement officials to seek out evidence for a criminal trial. Considering the accelerating crime rate in India, through this research paper, we focus on how they can be dealt with using Cyber forensics, Electronic Evidence and Investigation and how they can largely benefit crime investigation. After a careful review and study of employment figure from analysts, job boards globally, it has been estimated that there would be a proliferation of job openings in the field of cyber forensics in India. However at present, in India, it is just starting to get looked at due to several obstacles like slow adaptation to new technology and lack of economic resources that stand in the way of Digital Forensics which is reasoned in this paper. This study also includes exploration of the realm of digital forensics with its relevance in law and courts. The paper encompasses the observation of the type of data cyber forensics focuses on and brings into light, the latent demand for forensic services in India and different parts of India. Through this paper, we aim to promote interesting discussions in several emerging areas of digital forensics.

KEYWORDS: Evidence, Accelerating crime rate, Crime investigation, Job openings, Obstacles, Demand.

Crime Against Women In Cyber World

Vishal, Chandigarh University

Abstract

Cyber Crime against women in country like India reveals the loopholes in present laws and policies of the Indian judicial system and what can be done to ensure safety in

cyberspace. It shows how women become the soft target of trolling, online grooming, bullying, pornography, sexual defamation, morphing, spoofing and so on. Crime against women rise in all the fields being a victim of cybercrime could be most traumatic experience for a woman. Especially in India where the society looks down upon the women and the law doesn't even properly recognize cybercrimes. This paper will talk about the various types of cybercrimes that inflicted upon a women and how they affect her. I will briefly examine upon the laws that exist to protect the women in these type of cases such as the Information Technology Act (2000) and the new laws which are coming in this field such as the Criminal Amendment Bill (2013). I am going to take assistance of various reputed cases in cyber crime to reach on conclusion. (i.e. Mary Roy v. state of Kerala). We also have elaborate review upon increase in cybercrime on women's and its various causes. I will also suggest several remedies to counter the increasing cybercrime against women in our country.In conclusion I focus upon the various options which are available for the victims of the cybercrime and what are the changes required in legal system to effectively curb the rising spirit of cyber criminals.

Cyber Stalking

Richa Sharma & Harpreet Kaur , UILS, Chandigarh University

Abstract

In the era of cyber world as the usage become more popular, there was expansion in the growth of technology as well, and the term 'Cyber' become more familiar to the people. Social networking technology provides a social, collaborative and interactive platform for internet users. Users become more open in expressing their thoughts and sharing information, and along the way this contributes to the rise of violation. One of the violation faced by the internet users is cyber stalking. Cyber stalking in general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, leaving written messages objects. Cyber stalking victims experienced psychological and behavioral effects such as depression, isolation, anxiety and cautious of their surroundings. They collect all personal information about the victim. In facing the phenomenon they devolved strategies such as confiding with family members, close and trusted friends support. There are various psychological reasons behind stalking like jealousy, obsession and attraction, sexual harassment, revenge and hate. Cyber stalking is serious growing problem. There can be better co-ordination among various national and international agencies to make the system more efficient and information technology act, 2000 more secured and trustworthy. A positive effect of being cyber stalked is the tendency to be more alert during online, and careful in sharing their personal information through social networking sites and protect all accounts with password.

Role Of Uno For Preserving Peace And Security In Cyber Space

Kalpana Devi , Ph.D Research Scholar
Maharaja Agrasen University Baddi.

Abstract

Before discussing the fundamental role of United Nations towards the preservations of peace and security in cyber space, we should know about what exactly is cyber space? Cyberspace, unlike most computer terms, cyber space does not have a specific/definite

definition. It generally refers to a block of data floating around a computer system or network. Because of the advent of the internet cyber space now extends to the global network of computers as defined by Gibson: Cyber space is a consensual hallucination experienced daily by billions of legitimate operators in every nation. William Gibson is the one who used the word “Cyber space” for the first time in his book called “Neuromancer” written in 1984.
If we talk about the advantage of cyber space, like every other technological inventions, it also has so many advantages, for example, it is best source of information, social networking, entertainment, etc. But sadly some disadvantages outweigh the advantages as computers connects to the internet are very prone to targeted virus attacks and may end up crashing. The security and dangers are always entitled within. You never know who is accessing your personal information as given in your profiles by yourself and what they do with it. Likewise, National security is one of important issues relating to it. All the above points can be headed as **cyber insecurities**. The objective of my current writing is to focus on the various contributions and steps taken by United Nation organization for the preservation of peace and security in the cyber world. The paper will be covering the following points:

- Concept of ICT
- Transnational threats
- Human rights developments and Internet
- Various steps taken by UN General assembly’s first committee
- How UN Security council’s works for this
- Contributions of various Research committees to curb the problems.

Mitigating Cyber Security Issues In Mergers And Acquisitions – National And International Perspective

Saurabh Sood , Research Scholar,
National Law School of India University, Bengaluru.

Abstract

Mergers and acquisitions (M&A)in present day and age have to go through stringent procedural formalitiesto contain growing cyber security threats that accompanythem. The need of the hour therefore is the streamlining and enactment of newlaws and timely engagement with Regulators at domestic and international level. The three imperative issues central to any due diligence exercise in M&A dealsinclude data privacy, data breach and other cyber security issues.Discovery of the above-mentioned cyber security issues and other breaches pursuant to the M&A deal is quite common today wherein the parties are left in lurch. In majority of the cases, it was only post M&A transaction that the acquiring company found out cyber security issues. One such example is of an acquisition deal between Verizon and Yahoo wherein Verizon discovered about Yahoo’s cybersecurity and data breach issueafter the execution agreement was executed by Verizon for acquiring Yahoo.Unfortunately, cyber security risks during a cross border M&A deal for a number of reasons have always been under-emphasized and not made a part of the formal due diligence process. To gauge the relevance of including threats of cyber security to any cross-border M&A deal requires the fundamental understanding of present and evolving parameters of commercial reasonableness and makes the role of cyber experts is indispensable to any M&A deal.

Keywords – M&A, Cyber security, Data breach, Companies Act, 2013, Due Diligence,

The Bestiaity Against Children In Cyber Arena

Shaurya Dutt & Sheenam Thakur, Student ,
H.P. National Law University, Shimla

Abstract

"Childhood should be carefree, playing in the sun; not living a nightmare in the darkness of soul."

-Dave Pelzer

Violence against children and young people in cyberspace is a new phenomenon that will continue to affect more children and young people across diverse locations unless safety planning is built into the structure of so-called new information society. Cyberspace is a new social environment that is distinct and yet can encompass all the physical places in which people interact. The protection of children and young people in this environment is as essential as in any other location. But there are special challenges: Identifying potential harms, understanding the perspective of young people, and enacting practical measures to assure children of their right to protection. In this paper the authors strenuously try to elucidate about the responsibility that exists in the physical world to assure children and young people of their rights and protection also applies to cyberspace and the use of new ICTs.

Crimes Against Women Under Cyber Law

Shreya Saxena & Vanshika Yadav, Student,
B.A. LL.B. Lloyd Law College

Abstract

Being a sufferer of cybercrime could be the most agonizing experience for a woman. In this paper, we shall throw light on certain social, economic and political implications being observed globally in many forms such as spying websites like 'Wiki Leaks', hacking, trolling, email spamming and spoofing, cyber stalking, body shaming, cyber defamation, pornography and many such forms of indecent representation of women that are pervasive in the cyber world. This paper will contribute to the legal research on cybercrimes targeting women. We shall also address to some relevant penal laws like IT Act, 2000, The Indecent Representation of Women (Prohibition) Act, 1986, The Indian Penal Code, 1860 and take support of different cases related to it. Violence against women has led to the emergence of cybercrime as a growing worldwide problem with prospect significant societal consequences. In India as well as in other parts of the world the acts of cyber violence are increasing and taking diverse forms as evident from different online platforms and media reports. This paper will further examine the recent increase in cyber violence against women and its different causes and will suggest assorted remedies to retaliate the increase of cybercrimes against women globally. However, under this context the effect on a woman is more mental than physical and the laws ensuring women's security focuses more on physical harm than the mental one. Moreover, the present paper will also focus on introspecting the gap between cybercrimes against women and laws regarding the same.

Data Protection Bill, 2018 And Data Privacy: Whether The Focus On Protection Of Individual Right Is A Myth Or A Reality?

Dr. Garima Tiwari & Sumedha Ganjoo,
Bennett University, Greater Noida

Abstract

"Privacy is dead, and social media holds the smoking gun."- Pete Cashmore

In India, privacy until recently was assumed to be protected as a Fundamental Right and privacy though not explicitly set out in Indian Constitution has over time been read into Article 21. In hearing the PIL questioning the vires of the Aadhaar Scheme, the Government took a stand that privacy was not a Fundamental Right. In order to read privacy into Article 21, the Supreme Court referred the PIL to a larger bench. Considering that privacy is a human right and India has undertaken to protect it as such, specific legislation protecting this right and also clarity in reading this right into Article 21 is imperative. Therefore, in Govind v. State, Supreme Court read privacy into Article 21.

In today's world data collection is ubiquitous, so is data sharing. Google, Facebook etc., collect data and share data. These companies sell data to others, which use it for marketing, in what is known as targeted marketing based on social behaviour. Up until now, privacy laws in India offer little protection against misuse of personal information. The transfer of personal data is currently governed by Sensitive Personal Data and Information Rules, 2011 which has increasingly proved to be inadequate. There is a proposed Data Protection Bill, 2018 which makes individual consent pivotal to data sharing. The effects and consequences of this bill are yet to be seen. The paper would therefore, look into the broader contours of the Data Protection Bill 2018 and critically assess it in light of Article 21 and right to privacy.

Keywords- Privacy, Data Protection, Fundamental Rights, Social Media.

The Blockchain Technology : Future Globalization

Vipasha Ghangoria, Ph.D. Student, Dr. R.M.L.
National Law University, Lucknow

Abstract

In today's world, the states are aspiring for hegemony, power networks and attempting to make impregnable structures to defend data, as data is a valuable currency. This paper presents a comprehensive overview on Block chain that creates an aura of transparency as every block is a record of transaction providing unalterable, censorship resistant document of history and addresses the Byzantine Generals Problem. Since the global financial crisis 2008, the states have been attempting to tighten banking and financial activities. On the contrary, many people believe in more transparency and believe in empowering the public to intervene directly for the larger public interest. Recently, Facebook has announced Libra crypto currency, powered by the encrypted block chain technology which will change the landscape of banking. The Block chain technology also has multiple trade related applications encompassing a diverse set of areas related to World Trade Organization like finance, customs, transportation, logistics, insurance, government procurement, intellectual property fighting piracy and counterfeiting and so on. The technology is also penetrating into the e-commerce world. This paper discusses Block chain as a financially potent tool in the sustainable development of the global economy by reducing trade costs, facilitating participation of MSMEs in the international trade and solving data localization issues,

thereby bringing the world closer. This technology has the potential to bring Trade Globalization to another level. The financial services industry will benefit multiple folds from the growth of this technology combating cyber security risk and thereby protecting the integrity of the global financial system. The author provides the practical and legal implications of block chain on the international trade by studying the current challenges that are faced.

The existing IoT installations are often vulnerable and prone to privacy concerns. This paper studies the use of Block chain to strengthen the security of IoT networks through a resilient decentralized mechanism safeguarding critical security-related data. Ethereal, a Block chain based start up gives users an edge to control their data unlike other major servers where a lot of privacy has to be ceded. Recently, even an air and space program like NASA has proposed an Air Traffic Management Block chain featuring smart contract support and high bandwidth communication channel enabling secure and private communication with air traffic services, addressing privacy issues and spoofing. Due to the decentralized mechanism of Block chain, the hackers are denied access to the entire repositories of data and do not have a single point of entry.If we are able to create a conducive ecosystem using block chain, the international trade would become fundamentally different in the coming years. This paper is an effort to demonstrate the trailblazing usage of Block chain technology in multiple industrial applications. The author also gives an overview of the challenges in the block chain technology like limited scalability of block chains, energy consumption issues and proposes solutions to go forward.

Cyber Trolling: Why It Happens And How To Address It?

Upagya Sharma, Assistant Professor, H.P. College of Law,
Kala – Amb, District – Sirmour, H.P.

Abstract

Internet has revolutionised the world. The wide array of services and information available online boggles the mind. One can think of a hundred reasons for praising what the net has brought to us but at the same time one should not ignore the dark side of the web. In today's fast paced world, one way to re-connect with your family and friends is social networking sites. Also, micro-blogging websites provide you with the opportunity to send your views on current affairs around the globe, to the world at large in a single click. There are chat rooms where you can post your queries or your opinions without judgement as anonymity is virtually guaranteed on the web.Alas, this has given rise to the phenomenon of online trolling. Trolling is defined as creating discord on the internet by starting quarrels or upsetting people by posting inflammatory or off-topic messages in an online community. A social media troll is someone who purposely says something controversial in order to get a rise out of other users. Internet trolling is thoughtless, cruel, harmful, and can lead to some serious consequences such as depression, self-harm and sometimes even force the victims to contemplate and attempt suicide. This paper is an attempt to understand the phenomenon of online trolling, the reasons behind it, to determine if the laws of our country are equipped to tackle it and if not; then to find solutions so that we can be rid of the menace of trolling.

Legal Challenges In Cyber Law With Special Emphasis On Securities, Spam And Financial Fraud

Zeeshan Hasan & Syed Arsh Jamil Students B.A.LLB(Hons).
Faculty Of Law,Jamia Millia Islamia.

Abstract

The World is emerging day by day where cyber and internet is one of the major factor of its development and has become one of the most expanding & emerging sector of this era where a person's day to day work depends on it. The growth of various information and communication technology have made life easier and enhanced the mode of communications, its functioning and qualities of life, whereas on another side there are tremendous increase of various challenges and trends in cyber law and internet security. This research paper discusses about the various emerging challenges before cyber law in the field of cyber world from mobile law to social media from cyber security to cloud computing and various banking financial fraud. The current manuscript also discuss about the various legal provision along with the related case laws present to prevent the menace of cyber crime. The researcher also made the comparative analysis of different modes of prevention and attempt to provide a glimpse on challenges before cyber law.

Further the Research Paper discusses detailed statistical analysis of Cybercrime reports by National Crime Record Bureau (NCRB), challenges to cyber law and their protective measures to counter the ever increasing cybercrimes. At last, the conclusion is focused on the transformation required in the legitimate system and options available to the victims of cybercrime.

Key Words

Cyber Crime, Mobile Fraud, Media Challenges, Spam Law, Financial Fraud

Inconvenience Caused To The People Through Cyberspace By Netizens: An Overview Of Cyberspace

Dr. Pushpanjli Thapar, Assistant Professor, University Institute of Legal Studies
Ava-Lodge Campus, Shimla - 171004

Abstract

The term Cyberspace was first used by the cyberpunk science fiction author William Gibson, which he later described as an "Evocative and essentially meaningless" buzzword that could serve as a cipher for all his cybernetic musings. Now it is used to describe anything associated with computers, information technology, the internet and the diverse internet culture. Cyberspace is the electronic medium of computer networks in which online communication takes place and where individuals can interact, exchange ideas, share information, provide social support, conduct business, engage in political discussion and so on. It is readily identified with the interconnected information technology required to advice the wide range of system capabilities associated with the transport of communication, contact products and services. However, the term cyberspace is rooted in the science of cybernetics from the Greek (Kybernetics, Steersman, Governor, Pilot or Rudder) cyberspace is the place where telephonic conversation appears to occur. Cyberspace is a virtual space where internet works just like the real world comprises the entire earth. Cyberspace consists of the entire virtual world i.e. the world where people are connected through computer and internet, where computer programmes work and data is processed. The number of users of the internet

jumped to 700 million in 2001 from a mere 143 million users in 1998 with a USD 300 million. E-commerce websites on the IT gives the users the opportunity to decide what they want to see or hear. There are more than 120 million hosts worldwide of this one, huge and gigantic network. The people who are using cyberspace are called netizens and they have to strictly follow the norms and ethics of cyberspace. In the knowledge society of 21st century, it is difficult to escape from becoming netizens. To match with the society, we must know ethics. Norms, rules and regulations of cyberspace is called cyber law and is essential to create order in cyber space but today apart from positive side of e-revolution, there is a seamy side also and computer, internet and ICTs in the hands of criminals have become weapon of offence accordingly a new branch of Jurisprudence emerged to tackle the problem of e-commerce and of cyber crimes in cyberspace commonly known as cyber law or cyberspace law or information technology law. Many laws and amendments has been made like information technology amendment act 2000 before 2008 IT act for the first time. A model law on e-commerce on international trade and law (UNCITRAL) was further adopted by UN General Assembly by passing a resolution on 30th January, 1997. Further India was also a signatory to this model law and had to revise its national laws as per the said model law. Therefore India also enacted the IT Act, 2000, and then an amendment act 2008 was passed. But in India, section 75 of the IT Act, 2000 provides extra-territorial jurisdiction to the Indian courts as often need to assume jurisdiction over foreign subjects would arise with increase in activity on the internet.

Cyber Voyeurism: A Threat

Dr. Sangeeta Thakur, faculty member, UILS, Ava Lodge,
Chaura Maidan Shimla

Abstract

A person who derives sexual gratification from the covert observation of others as they undress or engage in sexual activities is called voyeur. The Indian Penal Code recognizes sexual harassment, stalking and voyeurism (watching a woman engaging in a private act where she would not have expected to be observed) as crimes. In this regard amendment was sought U/S 354C of IPC in the year 2013. It states that sexual voyeurism is a kind of sexual harassment that is identified under this Act. Voyeurism is an offence to both the dignity as well as the privacy of a person by infringing upon the right of individuals to control the exposure of their bodies without their consent or knowledge, either through distribution of images or videos against the wishes or knowledge of victim. Security in the cyber world is the most sensitive issue in the ambit of cyber laws. Security is directly linked to an individual's safety of their privacy and personal information. Internet usage has been increasing over the past few years and it has found its place in every home of common man. It has lead to an advancement in the technological world. It can be accessed through cell phones, televisions, computers or in any other electronic mode. Video voyeurism is a threat to the right of privacy as it reaches to every class of people within few seconds. It also hampers the safety and security of the individual and it is due to this reason that there was a need to bring up various laws for its protection. The privacy of the individual can only be protected by making the legal system strong and having a dedicated law framework. There must be stern punishments along with heavy fines. There are instances of CCTV cameras which were installed at a public place which captured

youngsters kissing each other and footages found their way to the internet. Though as per IT Act Sec 67 any owner of CCTV camera can be booked if camera captures obscene electronic information. With the increasing awareness it is hopeful that the government will consider privacy issues as a security concern for the country.

Cyber Victimization Of Women And Cyber Law In India

Lekh Raj And Sunil, Ph.D. Research Scholar, H.P.U. Summer Hill, Shimla-5.

Abstract

Rapid growth of the internet and computer technology over the past few years had led to the growth in new forms of crimes known as cyber crimes. Cyber crime is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offense. Cyber criminals may use computer technology to access personal information or use the Internet for exploitative or malicious purposes in various forms such as: Cyber-stalking, Harassment via e-mails, cyber defamation and cyber terrorism. Women are the most vulnerable targets on the internet and digital communication technology due to their gender and the consumability of image of women as porno materials. In India the situation is different from the Western societies, especially due to orthodox social norms. Cyber law is a term used to describe the legal issues related to use of technology, particularly 'cyberspace' i.e. the Internet. In India, the IT Act, 2000 as amended by the IT (Amendment) Act, 2008 and National Cyber Security Policy 2013 for combating cyber crimes. Indian laws are well drafted and capable of handling all kinds of challenges posed by cyber criminals. However the enforcement agencies are required to be well versed with changing technology and laws.

Keywords: cyber crimes, women victimization, cyber law.

Online Defamation And Women: A Curious Case Of #Me Too Movement

Mridul Surbhi, Assistant Professor, Sociology, University Institute Of Legal Studies, Himachal Pradesh University

Abstract

Online defamation is a nuisance, so much that the Indian Law deems it a criminal offence and an offender is liable to imprisonment up to 2 years. A woman ranging from teenage until she stays on any public platform, one time or another faces cyber bullying and defamation. Statistics point out that women are relatively more prone to cyber defamation and bullying than men. Misogyny, objectification, deep-rooted patriarchy and casual sexism have found another face…the Internet. Majority of our society unanimously agrees that women in this digital era are wronged and objectified more than ever. In the paper a special case is put under the microscope to examine the implication and possibly the utility of cyber defamation. Almost 2 years ago, a moment in the United States of America found an outlet to this built up anger of women against their perpetrators. The #Me Too Movement used the same weapon of cyber defamation to not only expose sexual misconduct by powerful and eminent personalities in different fields but also inspired millions of other women worldwide to come out and defame sexual predators online. In India too, the movement resulted in the accusation of dozens of men in politics, entertainment and the arts, with several prominent figures either resigning or being suspended as a result. Can online defamation also become a useful tool to

bring to light systemic abuse of women? Or by suing a woman for defamation, is our Law sending out a regressive message: that the fundamental right to life, safety and dignity of a sizeable section of the workforce does not matter?

Internet Addiction- Is It For Real?

By Dr.Akanksha Sud, Department Of Psychology H P.U. 171005

Abstract

Let's begin by understanding how technology affects our brain? The 1st indicator could be the disturbance in our sleep cycle. The 2nd our frequent forgetfulness and increased loss of attention followed most importantly by loss of our real identities when we are wrapped in our social images and social identities. Leading to Narcissistic &self absorbed personalities. Then there are the parents concern- about Internet addiction. Phone addiction. Technology addiction. Whatever you call it, a lot of parents are expressing worries that their children are addicted to their devices. Is the behavior that parents are concerned about really addiction?

Experts say that there are 5 types of Internet addiction so to say:

1. Cybersexual: Cybersex and Internet porn
2. Net compulsions: Online gambling, shopping, or stock trading
3. Cyber-relationships: Social media, online dating, and other virtual communication
4. Cyber-relationships: Social media, online dating, and other virtual communication
5. Information Seeking: Web surfing or database searches

Finally is internet addiction related to mental illness?

Studies do reveal that adolescents who struggle with Internet addiction often have other mental health problems like alcohol and substance use, depression, suicidal ideation, ADHD, phobias, schizophrenia, obsessive-compulsive disorder, and/or aggression

So lets ask ourselves: is Technology our Nemesis?

As technology continues to permeate nearly every avenue of our personal lives, It's become almost natural for us to blame technology for the stresses of modern life. Or on its own, is technology simply a powerful tool with the potential to increase our productivity, health, education, and happiness.

Consequences Of Crimes Against Women Under Cyber Law: Rights And Regulations

Dr.Nida Fatima, Department Of Political Science,
Aligarh Muslim University

Abstract

Despite the fact that crime against women is on a rise everywhere and being a victim of cybercrime could be most harrowing experience for a woman. Mainly in India where our society looks down upon the women and the law doesn't even properly be acquainted with cybercrimes. In this paper I am about to discuss upon the range of types of cybercrimes that can be imposed upon a women and how they unfavourably affect her. I shall also in a few words examine upon the different laws that stay alive to protect women in such cases such as the Information Technology Act (2000) and the new laws that are near-term in this field such as the Criminal Amendment Bill (2013). I will be taking assistance of various cases reputed

cases in cybercrime to arrive at my conclusion. I am also having a detailed evaluation upon the latest increase in cybercrime on women and it's a variety of causes.

I also plan to put forward several remedies to contradict the ever growing cybercrime against women in India. In my conclusion I will focus upon the options accessible to the sufferers to cybercrime and the changes essential in legal system to successfully restrain the rising spirits of cyber criminals.

Keywords: cyber crime, India, women, crime against women, Remedies

Emerging Challenges In Cyber Law

Ms. Vibhuti Nakta, Research Scholar, Panjab University
Ms. Ebani Mittan, Student, UILS, H.P. University

Abstract

The development of cyber space has created both delight and complexity in all walks of life. The scientific technological innovations have enhanced the mode of communication, functioning, quality of life and have become an inseparable part of life. Its significance it has enhanced the criminal activities, raised moral concerns and ethical dilemmas in the cyber space. It has raised concerns of cyberspace security, information protection, privacy, IPR issues, and electronic transactions. Cyberspace is a free space with minimal restrictions and advocates of cyber libertarianism claim for declaration of independence of cyberspace. However, the advocates of cyber paternalism emphasise the need for imposing restrictions, strict legislative provisions to curb the growing crimes and ethical violations in cyber space. The regulation of cyberspace is gloomy due to discrepancies in jurisdiction, subject matter, ethical challenges, anonymity, etc.

A Study On Online Cyber Crimes In India

Dr. Sanjeet Sharma, Assistant Professor,
Computer Sciences, UCBS Avalodge, HPU Shimla

Abstract

Cyber crimes are a recent class of crimes which is rapidly expanding due to extensive use of Information Technology. Many people take advantage of Information Technology to perform acts to satisfy their unfair needs. Online shopping and wide use of "social media" are important causes of cyber crimes in India. These crimes are taking place due to lack of awareness. Further, people do not complaint against these crimes to authorities. Moreover the complaints filed by the victims are not cleared within reasonable time period. This delay in dealing with the complaints leads to no registration of complaints. This is not favorable condition. The law IT (Information Technology) Act 2000 and several sections of the IPC are unable to control crimes caused by cyber world in country like India. In the present study impact of social media, trends towards shopping online and punishment for cyber attackers is evaluated. Lastly suggestions are provided to government and online shopping customers to deal with the cyber crimes.

Social Media And Cyber Terrorism

Dr.Pushpanjali Sood, Assistant Professor, University Institute Of Legal Studies,
Himachal Pradesh University, Shimla, Himachal Pradesh, India

Abstract

The social media has gained so importance nowadays that it seems that it is almost impossible to survive without it. The virtual world is replacing the real world to a great

extent. Discussions from the drawing room and offices are being shifted to social media. More information is being revealed by people on social media which has given space to criminal minds to commit crimes. When youngsters share sensitive information on social media without knowing that it can be used against them or sometime against public at large, which may result in cyber terrorism. The ICT (Information Communication & Technology) revolution has given rise to cyber terrorism, which has become a gruesome threat to combat, because of its intangible nature. By definition cyber terrorism means to damage information, computer systems and data that result in harm against non-combatant targets. India currently has the fastest growing user base for Facebook and Twitter, the two top social networking sites. With over 460 million internet users, India is the second largest online market, ranked only behind China. India is becoming increasingly vulnerable to this menace because of rapid digitization and proliferation of mobile data without matching pace of cyber security and cyber hygiene. At present, India is ranked third in terms of cybercrime incidents behind the United States and China. The paper discusses role of social media in cyber attacks and challenges faced by the Indian cyber security Industry.

Keywords: social media, digitization, cybercrime, cyber terrorism, cyber security.

Crime Against Children In Cyber World (Child Pornography, Sextortion, Indecent Representation)

Jyoti Kaushal and Tamanna Kohli, Student, BA.LLB (9th Semester,
Deptt. Of Laws,PURC, Ludhiana

Abstract

Children are the most important asset of every nation and every effort should be made to provide them equal opportunities for development so that they become robust citizens; physically fit, mentally alert and morally healthy endowed with the skills and motivations needed by the society. But it is unfortunate to see that child rights, child protection and child development have not been addressed in a comprehensive, sustained and effective manner. The crime against children which has assumed most terrifying proportions is child sexual abuse. The world has become a frightening place for the children, its manifestations are several, one of the emerging problem being online child sexual abuse. With new media technologies available at lower costs, online child sexual abuse has become a serious problem not only in India but all over the world. This paper will analyse the problem of child pornography, sextortion, paedophilia and other kinds of crimes among children online and the effective implementation of the present legislations in India with special reference to IT Act 2000.

KEYWORDS: child pornography, paedophilia, Information Technology, sexual abuse, cyber bullying, obscenity, child exploitation

Cyber Victimization Of Women And Cyber Law In India

Sunil Kumar, Ph.D. Research Scholar,
Department Of Public Administration, HPU, Shimla-5

Abstract

Rapid growth of the internet and computer technology over the past few years had led to the growth in new forms of crimes known as cyber crimes. Cyber crime is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offense.

Cyber criminals may use computer technology to access personal information or use the Internet for exploitative or malicious purposes in various forms such as: Cyber-stalking, Harassment via e-mails, cyber defamation and cyber terrorism. Women are the most vulnerable targets on the internet and digital communication technology due to their gender and the censurability of image of women as porno materials. In India the situation is different from the Western societies, especially due to orthodox social norms. Cyber law is a term used to describe the legal issues related to use of technology, particularly 'cyberspace' i.e. the Internet. In India, the IT Act, 2000 as amended by the IT (Amendment) Act, 2008 and National Cyber Security Policy 2013 for combating cyber crimes. Indian laws are well drafted and capable of handling all kinds of challenges posed by cyber criminals. However the enforcement agencies are required to be well versed with changing technology and laws.

Keywords: *cyber crimes, women victimization, cyber law.*

Digital Era: Security Of Women Infringed

Aswinikumar Bairagi, 5th Year Student, School Of Law,
Galgotias University

Abstract

This is undoubtedly a digital era. Most of the works are performed through internet. This internet makes our life easy. But also increases the crime in the society as well. As usual the females are targeted by the males in the society. Due to open access of internet, any data is uploaded then it is accessible through any part of the world. Any crime committed through internet that is covered as cyber crime. But it is very unfortunate that there is no proper definition for the term cyber crime till now.

The main of the paper is to discuss the law that governs the crimes committed in the internet and how the women get affected through that.

Crimes Against Women Under Cyber Law

Mukul Rathore , B.A. LL.B 4th Year Banasthali Vidhyapeeth

Abstract

Cybercrime is an evolving form of transnational crime.The major cybercrime put woman into depression, hypertension and suffer from anxiety due to e-harassment. Most common cybercrimes are cyber-stalking, defamation, morphing, cyber pornography, trolling etc.Though crime against women is on a rise in all fields being a victim of cybercrime could be most traumatic experience for a woman. Especially in India where the society looks down upon the women, and the law doesn`t even properly recognise cybercrimes. I shall examine upon the various laws that exist to protect women in such cases such as the Information Technology Act (2000) and the new laws that are coming upon in this field such as the Criminal Amendment Bill (2013).

Cyberspace Governance With Special Reference To Online Gaming In India

Shivanshi Thakur & Kalyani Acharya .
Research Scholars, H. P. University, Shimla

Abstract

Cyberspace is certainly different from terrestrial space where social control is informal. While the Internet has transformed our world with online information, interaction

and alliance, online addiction has also been introduced by it. Its governance requires pluralistic endeavour, firstly to define it i.e. what constitutes it and then effective policies and laws to secure it. Online gaming is like Small Island in a huge ocean of cyberspace which is expected to be one billion dollar industry by 2021 in India. Online gaming is of different kinds and creeds but generally prevalent these days are Massively Multiplayer Online Game (MMOG) that allows million users to interact in one gaming environment. It is indeed giving a platform to cybercriminals to misuse it in the form of various offences like cyber bullying, swatting, sexual offences, online child grooming and many more against children and the youth. India has not yet recognized the acuteness of online game and failed to provide a regulatory framework for its governance. This paper is an attempt that will indeed define the arena of online gaming and crime associated with it. Also, most importantly this paper will provide regulatory frame work by self regulation in the form of a Commission which will regulate the age of players, timings etc. related to online games and governmental regulation in the form of legislation which will deal with the laws, crimes and other requirements.

Cyber Security In Banking Sector

Monika Parmar, Research Scholar,
Department of Economics HPU, Shimla

Abstract

Banking sector plays an important role for the economic development of the country. They not only act as the custodian of the wealth of the country but also as resources of the country. The general role of commercial banks is to provide financial services to general public and business, ensuring economic and social stability and sustainable growth of the economy. Now the definition of banks has been changed now because of introduction of technology advancement. Introduction of information technology has introduced new innovations in the product and now focus has shifted from class banking to mass banking. Now a day's all activities related to banks have been done through online whether its deposits or withdrawals of cash, loan or anything else which makes our life simpler. A rapid growth has been observed in the adoption of new security measures and transfers to the digital channels by Indian banks after 2010. The use of Information Technology by banks and their constituents has grown rapidly and is now become an integral part of the operational strategies of banks which makes a noticeable shift in the banking industry in the way customers deal with their transactions. There is a rapid increase in the usage of digital channels such as internet banking, digital wallets, mobile banking, ATMs in banking sector. The introduction of technological solutions have brought in convenience to the customers and cost effectiveness from the banking perspective but in the same time banks are highly obliged to maintain integrity of financial transactions and protecting the privacy of customers because everything has some pros and cons. No doubt, introduction of technological advancement is blessing to the sector but the adoption of these technologies has brought in a large number of information security threats in all sector and banking sector is the most vulnerable to cyber threat which may cause financial liabilities to the banks. With the rise in digital transactions and their spread to the country, cyber frauds like direct money siphoning from banks through phishing attacks, cloning, stealing of payment cards, identities and information etc are on the rise. The volume of cyber fraud at banks has doubled year after year. In 2017-18, cyber

frauds at banks saw a big spike over the previous year. According to a report by the Reserve Bank of India, a total of 2,059 cases of cyber fraud were reported in 2017-18 amounting to Rs 109.6 crore. The number of cyber fraud cases in 2016-17 was 1,372 amounting to Rs 42.3 crore.

Cyber Terrorism And Cyber Warfare

Ms.Shwetima Dogra, Ms.Priyanka Bhatoia
Student of Himachal Institute Of Legal Studies, Dharamshala (H.P)

Abstract

Cyber warfare is the most dangerous form of attack on any of the country or an organization which will paralyze all their activities as in this advanced world where everyone is dependent on the internet or all the actions are now online. If some country is being attacked in this form of attack, they will then automatically loose the battle before it starts to begin.

All their equipments will get defunct and then they will not be able to fight. Therefore they need to be protected from this. Cyber terrorism is also adopting this kind of medium to terrorize the people by threatening them to lose their money, kidnapping them and killing the people. Likewise, the example is like bit money (cash), or we can say online games which prompt them to kill themselves only. So to curb or to get protected from such kind of activities, there are number of guidelines given or warnings which are given from time to time to beware of these things. The proactive actions are taken at all the level so that there is no such loss. There are people who work day and night just to save the organization from such kind of warfares. That is why such internet activities are watched and being monitored, and likewise the phones are tapped to keep vigil on such kind of people all around the world. Hence the threat is not only from outside the country but also within the country itself.

Cyber Defamation In India: Anonymity & Jurisdictional Issues

Dr. Vijay Chaudhary, Assistant Professor,
H.P. University Institute of Legal Studies, Ava Lodge, Shimla-4.

Abstract

The rapid growth of the information and communication technology has brought great changes to our day today lives. And with the advent of numerous kinds of internet communications such as web blogs, e-mails, chat groups, social media platforms and many others, internet users are able to easily publish and disseminate any kind of information to the public at large. With the tremendous rise in the use of the internet as a medium of communication, chances of use of the web as a medium for publication of defamatory content by unscrupulous individuals has increased multifold and there is a need for a clear, coherent expression of the law in this area. While the need for a uniform law to govern internet transactions is undoubted, the question is whether the traditional law of defamation can be applied to the internet without any changes. Furthermore, the law of defamation requires a delicate balance between the right of persons not to be defamed and the right of freedom of speech and expression of others, which is difficult to maintain in the cyber world. Since internet allows transactions between persons of various jurisdictions, an international agreement is required for any regulation governing defamation over the internet. The present paper focuses on examining the efficacy of the existing legal mechanism that governs such a

crime. Finally, this paper also attempts to highlight the loopholes/lacunae in the existing legal framework in India and possible suggestions and recommendation as part of its conclusion.

KEYWORDS: Cyber Defamation, Law, Anonymity, Jurisdiction.

Offences & Penalties Under The Information Technology Act, 2000

Priyam Kohli, Asst. Professor UILS, Shimla

Abstract

In today's fast and progressive world Computer has become an integral part of our daily routine, also to add and boost its capacities the introduction of the internet has brought a tremendous changes in our lives. People of all fields whether corporate, businessman or households are increasingly using the computers to create, transmit and store information in the electronic form instead of the traditional papers or documents as Information stored in electronic form has many advantages which has made the life of people much easier and faster than before. Despite of all the above stated advantages of computer and internet, we also can't deny of the fact that though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection.

Cyber offences are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. Cyber crime usually includes unauthorized access of the computers, data diddling, virus/worms attack, theft of computer system, hacking, denial of attacks, physically damaging computer system, internet time theft etc.

The increase rate computer usage with internet and the use of ever expanding and changing technology in computers has led to enactment of Information Technology Act 2000. The converting of the paper work into electronic records, the storage of the electronic data, has led tremendous changed the scenario of the country. Since new-new technology come every day, the offences has also increased therefore the IT Act 2000 need to be amended in order to include those offences which are now not included in the Act. Although there are new amendments to the Information Technology Act, 2000 that have been passed by the Lok Sabha , but they deserve a careful reading and a lot more is required to be done in this context.

Cyber Violence Against Women And Emerging Challenges

Apoorv Kumar, Shudhanshu Mani Tripathi,, B.Sc (Hons.) Forensic Science, Bundelkhand University, Jhansi,
Manvi Raj B.com LL.B (Hons.), 3rd year, Amity University, Lucknow,

Abstract

India being the largest democracy, known with high crime rate, loopholes and hand full of corrupted people. This old system requires changes for decreasing the crime rate out of which the fastest emerging crime is cybercrime. This generation is competent of the technologies. Any inappropriate happening on the digital world can be classified into Cybercrime. The Information Technology Act, 2000, is the act that deals with Cybercrime.

Historically, India being the land where women have special status, and they are the targeted too. According to the data of National Crime Report Bureau, the year 2016, out of 12317

cases, 21.9% cases were reported by the women. There are number of cases but only few are reported and there are majority of cases which go unregistered with justice being nullified. The reason for cases going unregistered is the unawareness of cyber-crimes on a specific platform, whereas other reasons being shyness fear of parents in teenagers and defamation in society.

Increasing crimes of cyber bullying & harassment, financial extortion, personal security theft, photo morphing, illegal sharing, fake accounts, etc are on a rise in our virtual world, which is going to cost a lot to the civilization. Great challenges are ahead because the weapons aren't guns anymore; they attack with computer, internet and passwords. Therefore, this paper focuses on the issues of the cyber law and crimes with special emphasis on Cyber Violence against Women and Emerging Challenges.

Keywords: Cyber-Crime, Digital World, Women, Defamation .

Cyber Pornography: The Menace Of Technology

Dr. MandeepVerma & Dimple Jishtu, Assistant Professor,
School of Law, Bahra University, Shimla Hills,Waknaghat, District Solan (H.P).

Abstract

WITH THE ACCESS TO INTERNET, Cyber Pornography is increasing every moment. In a click on internet different kinds of pornographic material appears on different formats. Cyber Pornography is pornography that is circulated through the internet. Internet has provided a medium for facilitation of the pornography. Viewing pornographic material on internet not only cause violence against women, but the material itself is violence against women. It lowers or diminishes the status of a woman as well as damages mutual respect between genders. Women are being presented as sexual objects/Commodities, therefore, boost the perpetrators of crime. Sexual violence against women, child abuse, juvenile delinquency etc. is the adverse effects of pornographic material. In India Cyber pornography has been covered by the Information Technology Act, 2000 to a certain extent. Along with Information Technology Act, the perpetrator can also be punished under various Sections of the IPC. However, The Information Technology (Amendment) Act,2008 introduced the provisions related to restraining pornography (*Child pornography*) but the law in our country is not adequate to meet the challenge of regulating the use of the internet to prevent dissemination of pornographic materials as observed by the Courts. The Paper examines this complex issue in a scientific manner and suggests viable solution for countering pornographic sites.

Key Words*: Internet, Pornography, IPC, Information Technology etc.*

Cyber Crime Against Women

Rajni Kumari Research Scholar,
Department of Political Science, HPU, Shimla

Abstract

We live in the world of science and technology. By technology our life became very comfortable. There have been numerous technological advancement and crime developed the last decade. In which cyber crime are most famous. In simple way we can say that cyber crime is unlawful act against the computer. In which using a computer to attack other computers e.g. hacking, virus, worm attacks DOS attack etc. To solve these problems cyber law is formed. Cyber law is a term used to describe the legal i8ssues related to use of communication, technology, particularly cyber space. Through crime against women is on a

rise in all fields being a victim of cyber crime could be must traumatic experience for a women. Especially in India, where the society looks down upon the women, and the law doesn't even properly recognized cybercrime. In this paper I will discuss upon the various types of cyber crimes regarding women and how they adversely effect her. I shall also briefly examine upon the various law that exist to protect women. I also suggest several remedies to counter the ever increasing cyber crime against women in India.

Cyber Crime And Sustainable Development

Annpurna Research Scholar,
Department of Political Science, HPU, Shimla

Abstract

Cyber crime is also called computer crime. In a simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crime involves criminal activities that are traditional in nature. Such as theft, fraud, forgery, defamation and mischief all of which are subject of the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the information technology act, 2000. In cyber crime computer is used as a target or weapon to commit real world crime e.g. hacking, cyber terrorism IPR violations, credit card frauds, pornography, sexual exploitation of women and children. There is no specific sustainable development goal to address cyber crime. It can be seen as an obstacle to achieving a number of targets. In September 2015 UN General Assembly has formerly adopted the universal integrated and transformative 2030 agenda for sustainable development a set of 17 sustainable development goals. These goals are to be implemented and achieved in every country from the year 2016 to 2030. The 2030 agenda for sustainable development clearly confirms that without peace there can be no sustainable development and there is no peace. Reducing conflict, crime, violence, discrimination, stable conditions are key elements of people's that are essential for sustainable development. Under these goals all countries went to promote a peaceful and sustainable society. Thus present paper explains the cyber crime's impact on sustainable development.

Secure Payment Using Mobile Wallet Framework For A Mobile Commerce Application

Sunil Mankotia, UCBS, Ava Lodge, Shimla

Abstract

In today's world the mobile devices and smart phones are used heavily and have become one of the most essential requisite of everyday life. The development of several applications feasible for those devices has revealed that there is a huge demand for applications of mobile. However one similar issue which entire devices share must be solved still namely the restricted device capability regarding feasible resources like the power of processor, consumption of energy and available memory. A technology which aroused in the IT sector provides an opportunity to solve those issues namely the mobile computing and cloud computing. The present research paper focuses on developing an M-Commerce application for secure transaction which consists of option selection by user, encryption using AES algorithm, sending of encrypted parameters to the user and generation of the hash value. The application is implemented and validated in Java platform. Several parameters were evaluated in the performance evaluation section which are i) set up time, ii) key generation time, and

iii) encryption time. The comparative results are obtained for the proposed system and the existing system to verify the superiority of the proposed system.

Crime Against Women In Cyber Law

Geetika Kaushal, Student, BALLB [5th sem.]
Indian Institute of Legal Studies, NLU,Ghanahatti

Abstract

Cyber crimes or computer oriented crimes are the crimes that involves a computer and network, the computer may have been used in the commission of a crime or it may be the target. Cyber crimes are defined as those crimes which are committed against individual or a group of individuals with a criminal motive to intentionally harm the reputation of the victim or to cause physical or mental harm, or loss to the victim directly using modern telecommunication network such as internet.

Cyber crime against woman is on at alarming stage and it may lead a major threat to the security of a person as a whole. Being a victim of cyber crime could be more traumatic experience for women. The cyber crime against the woman are : Harassment via email are the main offence against the woman in cyberspace, Hacking related activities may not always in restricted to the crimes committed against the nation or the corporate entities alone but sometimes it may be seen as a crime of any female victim to access her personal information including pictures without proper authorization with intention to misuse it, distribute it in the internet, modify a content and give a false impression of the victim are also criminal activities or cyber crime against woman like stalking and bullying. In India, the cyber crime against woman include sexual crimes and sexual abuses on the internet. India is considered as one of the few countries to enact IT Act to combat cybercrimes.

My article will give detail information about all above mentioned probelms or cyber crimes against women and also about the various legislations in India for preventing these crimes, It will also describe or explain the judicial approach in India regarding the topic by mentioning some case laws like Ritu Kohli case. This article also attempts to find out various reasons behind the fact as to why women are being victimized of cyber crime and at the end, I will conclude it by giving some suggestion about how these crimes can be prevented.

Cyberspace Addiction And Loneliness

Pankhuri Bhatnagar, Faculty ember,
University Institute Of Legal Studies, Himachal Pradesh University

Abstract

Cyberspace activity has become one of the most popular activities among the youth in the past decade. Cyberspace has become a world unto itself. However, excessive indulgence in the cyber world has led to its pathological use. Therefore, it is imperative to explore the consequences of "Cyberspace Addiction" - a behavioural addiction to virtual realms of experience created through internet. People become "addicted" to the internet, and often use it as an escape from their real life. Their face to face interaction with the people who are actually there in the real world around them starts declining. This can dangerously affect their social connectedness and hence may lead them to feel more lonely and secluded from the real world and people around them. Thus, the present study is aimed at determining the relationship between internet addiction and loneliness among the youth. 50 participants, ranging from 18-26 years of age, took part in the present study. In order to see the

relationship between loneliness and Internet addiction, Internet Addiction Test (IAT) developed by Dr. Kimberley S. Young (1998), and UCLA Loneliness Scale developed by D. Russel, (1996) were used. The results revealed that there is a positive correlation between loneliness and Internet addiction. Higher the Internet addiction higher was the loneliness.

Keywords: cyberspace, internet addiction, loneliness

Old Code, New Crime

Akshya & Yugansh Mittal, Law Researcher, Delhi High Court,
Law Researcher Delhi High Court

Abstract

The scenario and forms of Cyber-crimes have undergone significant metamorphosis due to the advancement of technology and tremendous growth observed in the internet user base globally. Cyber-crime being a complex problem encountered by countries worldwide raises various complications, snags and difficulties due to its borderless and anonymous nature. In this work, the emphasis is to sensitize the readers towards the newfangled category of Cyber-crimes and essential judicial precedents. The mainstream focus in this work is India with references from other Countries.

Challenges In Cyber Security Of 21st Century

Shivam Swaraj, Megha Aggarwal & Suhail Ahmad Khan,
B.Sc. (Hons) Forensic Science, 2nd Year, Bundelkhand University, Jhansi

Abstract

Cyber-attack is the most familiar word known in the dark era of emerging cyber-crime, so to overcome with this threat cyber security has played a vital role and has made all its possible efforts to secure internet. Cyber security is the science of protecting and securing the various data, programs or devices from cyber-attacks and mainly the institutions, organizations and the employees are targeted. The main prospective of cyber security is to secure the internet, web browser and World Wide Web. According to National Crime Record Bureau, India which released its annual report of crime data about 12317 cyber-crime cases were registered in 2016, about 6% rise as compared to 2015.Through Information Technology Act 2000, Government of India imposed various sections against cyber-attacks like sec 69, failure of decryption of data sec 70, securing access to a protected system stated that cyber-attack is an offence.

The present paper give detail about various challenges in cyber security against cyber-attacks. An awareness and basic understanding of the threats such as phishing, ransomware, security breach etc. posed in cyber world which will help in protecting the digital assets, intellectual properties. This paper also focuses on the cases registered at large scale.

Keywords: Data Breach, Decryption Of Data, Cyber-Attack

Cyber Victimization Of Women: A Study Of Legal Protection To Women Cyber Victims In India

Reetika Rana, Assistant Professor, UILS, Shimla

Abstract

In the age of internet and computers we have gained manifolds advantages in terms of efficiency and management but it has also brought to the front many negative effects and disadvantages. The crime using internet has also widened its roots in all directions. The cyber-crimes pose a great threat to individuals. Cyber-crime is a global phenomenon and

women are the soft targets of this new form of crime. Being a victim of Cyber crime could be the most traumatic experience for a woman especially in India where the society looks down upon the women and the law doesn't even properly recognizes cybercrimes. The paper delves upon the various types of cybercrimes that can be inflicted upon women. Further, the paper examines the various laws that exist in country to protect women against cyber crimes such as the Indian Penal Code, 1860, Information Technology Act, 2000. At the conclusion paper will focus upon the options available to the victims to cybercrime and the changes required in legal system to effectively curb the rising spirits of cyber criminals.

Keywords: women, cyber crime, crime against women.

Crime Against Children In Cyber World (Child Pornography, Sex Extortion, Indecent Representation)

Dr. Kuldeep Chand, Associate Professor, School of Law,
Maharaja Agrasen University, Solan

Abstract

Crime against children and young people in relation to new technologies, and in particular the Internet, is a new phenomenon that has spread across diverse societies in recent years in step with the emergence of several new technologies into the mass consumer market of many countries. A crime against children is a pervasive phenomenon that knows no political, cultural, economic, nor technological boundaries. The boom in information and communication technologies (ICTs) over recent decades has brought completely new ways of establishing and maintaining relationships. This is a very normal everyday reality for many children and young people, and an exciting possibility for the rest. In very different ways, children are vulnerable to multiple forms of violence that threaten their physical and psychological integrity. And just as in the physical world, a framework to protect children in cyberspace must be established which is based on child rights and human rights instruments. The scale of Crimes against children in virtual space is closely related to the rapid expansion of information and communication technologies (ICTs) since the early 1990s when the emergence of web browsers triggered the Internet boom. The Internet is perhaps the first and best known of the modern ICTs. In many ways, the subsequent development of other such technologies coheres around or depends to some degree on the Internet, which links in with several distinct technologies, including the World Wide Web, instant messaging (IM), chat rooms, online games, and file-sharing or peer-to-peer software.

Artificial Intelligence- Upcoming Cyber Security Officer

Abhishek Srivastava, B.Sc. (Hons.) Forensic Science II Year,
Dr.A.P.J Abdul Kalam Institute of Forensic Science &
Criminology, Bundelkhand University, Jhansi

ABSTRACT

Protection and guard to the digital databases is first initial step taken to prevent in increasing cyber crime rate, which is increasing day by day. We need an advance guard which can detect predict & respond to cyber threats. Capgemini Research Institute is reinventing cyber security with artificial intelligence which is capable of preventing & defending against cyber threats. AI is developing with the innovation and development in the field, its capability of detection, prediction & ability to respond against cyber threats cannot

be neglected.69% of enterprises from countries believe Artificial Intelligence will be necessary to respond to cyber dealts.

Fraud detection, malware detection, intrusion detection, securing risk in a network and user machine behavioural analysis are five highest Artificial Intelligence use cases for improving cyber security.

Keywords: Malware, Artificial intelligence, Innovation, cyber deaths.

Crimes of Social Media: The Faceless Evil of Cyber Harassment and Bullying

Meghna Thakur, Student (BA.L.L.B)
Himachal Pradesh University Institute of Legal Studies, Shimla

Abstract

Today the world has indeed become a global village. Almost everyone has access to a smart phone, computer, tablet or any other device with internet connectivity which allows them to connect with the rest of the world. Internet data plans are available at cheap rates, which has led to an increase in the number of cybercrimes being committed and reported. India in particular has not only bagged one of the top ranks for having the highest number of internet users, but we also ace the statistics of global sexual harassment. In 2018, a survey was conducted by Forbes in which a total of 37% of parents across India said their child was bullied online, with 14% of that total saying that bullying occurred on regular basis, making India a country of cyber bullies. With increased interconnectivity people have also started using social media more actively, this is evident by the fact that in 2012 Instagram had 35 million monthly active users and in 2019 this number increased to 1 billion. This research paper aims to study the:-

- social media usage patterns and habits of youth,
- the most commonly observed pattern of harassment and bullying on social media,
- reasons why most of the cases go unreported or are not taken seriously and some suggestions for the same.

KEYWORDS: social media, cyber-crimes, cyber harassment, cyber bullying.

Exploring Fairness In Indian E- Commerce From Competition Law Perspective

Dr. Gurujit Singh, Assistant Professor, Mr. Abhay Pratap Singh,
4th Year Student, University School of Law & Legal Studies,
GGSIP University, New Delhi

Abstract

This paper offers a normative studies of E- Commerce from the perspective of Competition Law in India. As it evident to all of us, how Internet evolved our lifestyle experiential changes from bricks-and-mortar retail shops to online retail portals (**ORP/ORPs**), everything is available through internet but at the same time, even on the online market to protect the interest of consumer as well as sustain the competition in the market will the foremost priority of the Adjudicatory Authority. Authors in this paper discusses the some key features of Indian Competition Law like Relevant Market, Exclusive Agreements, Predatory Pricing & Market Operation Price and their appreciable adverse effect on competition (**AAEC**) in the reference of ORPs with the help relevant Indian case studies. Further, discusses the relevant market in the vein of ORPs is just a channel of distribution to the relevant market or a separate relevant product market.

This paper examines the legal impact of the competition law on the E- commerce market to protect the interest of consumers and to foster and assist the competition in E-Commerce. This paper will rely on various reports and other instruments of legal and doctrinal research.
Keywords : E - Commerce, Competition Law, Online Retail Portals, Appreciable Adverse Effect on Competition (AAEC)

Fake Identities In Social Media: Teenagers And Social Media

Sohail Khan, Student, UILS, Shimla

Abstract

Now day's use of Social media has become common in our daily life such as Instagram, Facebook and Twitter. Due to excessive usage of social media there comes major problems like fake identities, cyber terrorism, crime against women and children etc are example of such criminal activity. There are some malicious users who steal pictures of females and make fake identities to commit fraud, earning money and e fool people. If you are way too careless then you may become a victim of sextortion where a stranger can blackmail you on the basis of your private picture that you have willingly or unwillingly shared with them. I made a fake account just for my research where I found that people themselves send request and try to have conversation with a stranger. In this digital world we have 500+ friends on facebook but not one genuine friend in a real world. Just for some followers we accept request of strangers and share with them our personal information. The purpose of the research is to discuss the behaviour of people on social media and offences related to fake profile. Here I propose to conduct a survey on teenagers and social media and try to find out effect of social media on their lives.
Keywords: social media, fake identities, sextortion.

Cyberstalking: A Phenomenon Of Mental Assault On Women

Payal Dhiman, Student, University Institute Of Legal Studies, Chaura Maidan,

Abstract

The development of internet technology in the present day world has given space for the development of crime such a crime is known as cyber crime which has widened its roots in all the directions. Stalking is a problem that both men and women are familiar with, but most of the victims are womens. Stalking is a form of mental assault, in which the perpetrators repeatedly and disruptively breaks into the life of -world of victim with whom he has no relationship, has a relationship, has no longer any relationship. Recent advancement in internet technologies has lead stalking to become cyber. In other words since these problems can occur on internet as well, it takes the form of Cyberstalking or online harassment. Cyberstalking is the act persistent and unwanted contact from someone online. Cases of Cyberstalking can often begin as seemingly harmless interaction. Sometimes, especially at the beginning a few strange more like unpleasant messages. But there is more to it perpetrators can monitor victims through various means. The advanced technology helps the stalkers to harass their target from any part of the world. USA is on the top of the list when it comes to the list of mostly affected country from the evil called cyber stalking .The victims are mostly teenagers.

Though for many people Cyberstalking may seem as an harmless act but it is dangerous in nature and can create havoc with the life and psyche of the victim. The purpose of this

research is to create awareness and to understand the reason behind why Cyberstalking happens? Cases relating to it, its legal recognition for and suggestions for its improvement would also be discussed.

Keywords : Cyberstalking, technology, perpetrators, Cybercrime.

Deep Web: The Invisible Domain Of The Cyber World

Dr. Gitanjali Thapar, Assistant Professor of English, UILS, Shimla

Abstract

The internet is just like an iceberg, the tip of the iceberg that is the 'surface web' is visible to the user which consists of billions and trillions of web pages. Beneath lays the invisible web that is not indexed and cannot be accessed by the conventional search engines. It is the 'Deep Web', which plays a central role in the development and proliferation of cyber crimes. It is in this dark and deep expanse of the World Wide Web that anonymity exists in many forms and paves way to cyber crimes and illicit activities. The Deep web or the hidden internet has an encrypted network and is accessible through the browser known as 'Tor' or the onion router. Tor is an internet networking protocol which conceals its user's identity and their online activities. This software allows its users to remain anonymous. The Deep Web has all the web pages that are unidentifiable by search engines and the Dark-Web refers to the sites where illegal activities take place with illegal content. This also includes trading sites where users can sell and purchase illicit goods and services. The entire transactions on the Dark-Web are done through the crypto currency like Bitcoin and Litecoin which are used as a trade link on the internet. The present article attempts to expound on the outrageous content available on the dark web. The paper also brings to the fore the crimes committed on the Dark-Web like drugs deal, stolen information, banking frauds and other crimes which are difficult to curb because of anonymity that governs the Deep Web.

Key Words:-Deep Web, Tor, Crypto Currency, Bitcoin, Litecoin, Onion Router.

Cyber Crime Against Women

Aishwarya Kashyap, Student, B.A.LL.B. (Hons) Semester-I, U.I.L.S., Shimla

Abstract

Today the entire world is connected with the internet. As life without it is impossible. The internet is considered as the storehouse of information. Due to advancement in the Information Technology sector cyber crimes are in increasing day by day posing a great threat to people especially women. There are many crimes against women like privacy infringement, pornography, sexual defamation, morphing, spoofing, etc. Women are considered to be the most vulnerable target of cyber crime. In this paper the author will focus on the different cyber crimes against women, their prevention and remedial measures .The difference of WO between a man and a woman is a minor one, but is a great source of threat to women. Steps like setting up crisis response centres in 100 districts , introducing "women only" buses in cities and removing jurisdiction boundaries for police in registering criminal cases should be incorporated. Putting in place a nationwide three-digit number [such as 100} to respond to all emergency situations on the lines of 911or 990 Emergency Management Systems in vogue in several developed countries and launching a sustained media campaign plan comprising measures to prevent crime against women.

KEYWORDS- cyber crime, women, internet, threat, Information Technology.

Cyber Security – Laws And Policy In India And Of Other Countries

Raman Kishore, BA.LLB 5th , I.I.L.S. Ghanahatti, Shimla.

Abstract

The world is the fastest revolution ever after the Industrial and green revolution and the revolution is digital revolution with digital revolution making its own space in the virtual areas at a fast pace. The human mind is being captured by it at a much faster pace. It is noteworthy that with the advent of this revolution today, but at the same time, it is posing threats to the mankind in a way that every second, we are prone to morenumber of risk. the same mouse which provides us with plethora of Information is infringing with our privacy and putting us into danger every now and then.

In this paper we discuss about the different types of cyber security issues and tries to address the issues by providing the various techniques for ensuring Cyber Security.

Cyber Security, which basically encompasses the various process techniques and controls which are designed to protect system, data and network from any kind of Cyber attack, is becoming challenge.

Cyber Security, Computer security is the protection of computer system from the theft of or damage to their hardware, software, electric data as well as from the disruption or misdirection of services they provides.

Due to its, complexity, both in terms of politics and technology cyber security is also one of the major challenges in the Contemporary world.

Cyber security refers to set of techniques used to protect the integrity of an organization' security architecture and safeguard its data against attack, damages or unauthorised access.

Cyber Attack And Need For Preparedness

Dr. Meera, Faculty member, UILS ,Shimla

Abstract

Cybercrime has increased considerably in the digital world. This harmful phenomenon, which is none other than cyber attacks, cyber threats, cyber wars, cyber threats, etc., pose enough problems for the security of States, organizations, individuals and, above all, the digital economy. The first instance of kinetic force used in response to a cyber-attack resulting in the loss of human life was observed on May 5, 2019, when the Israel Defense Forces targeted and destroyed a building associated with an on-going cyber-attack. This paper provides a broad knowledge of cyber-attack, cyber threat, threat categories, and their nature to provide data on preventive methods for cyber security, and offensive methods in cyberspace. All sorts of data whether it is government, corporate, or personal need high security; however, some of the data, which belongs to the government defense system, banks, defence research and development organization, etc. are highly confidential and even small amount of negligence to these data may cause great damage to the whole nation. Therefore, such data need security at a very high level. A number of countries conduct exercise to increase preparedness and explore the strategy, tactics and operations involved in conducting and defending against cyber attacks against nations, this is typically done in the form of war games**.**

Keywords: Cyber security, cyber war, cyber-attacks, cyber threat, cyber Offensive-defensive, preventive approach, preparedness.

Crimes Of Social Networking Sites

P.B. Adithya Sai & Ashwath Ethiraj, School of Law, Vistas Chennai

Abstract

It is a truth that every coin has two sides , same for internet it has both advantage and disadvantage. One of the most important disadvantage of internet is the Cyber Crime offence. The Social Networking Sites have created an era in the history of Cyber Space influencing netizens in their Personal sphere as well as professional level. The growth and impact of their websites at the exponential rate have attracted the cyber offender to commit Cyber Crimes in social medias. The Cyber offender are committing offence related to Privacy, Defamation, Misrepresentation of Identity, Obscenity and pornography, Sending offensive Messages, Cyber Terrorism and so on. In India most of the Cyber crime is committed by persons who are well equipped with cyber knowledge affecting the common internet users. In this paper tries to discussed various categories of cyber crimes which is based on social networking sites. This paper also suggested the various preventive measures against these unlawful acts in day to day life.

Keywords: Cyber Crime, Social Media, Cyber Law, Cyber Space, Legal Provision, Punishment, Preventions.

Cyber Crimes: Threat To Privacy

Shreya Verma, Student, HPUILS, Shimla

Abstract

Today's age is the age known as the Cyber age. Everyone is involved in some kind of online platform. And for enrolling in such web applications you need to provide a set of your personal information. Such information can be misappropriated easily leading to fraud, inconvenience, faking identities for committing crimes etc. . Such issues are increasing day by day leading to increased numbers of cyber crimes. The cyber laws made for coping up with such crimes are insufficient and lacking. The IT Act, 2000 has not clearly mentioned any rules or regulations regarding securing the private information of people. Our information is not safe and it can lead to various cyber crimes for which we have no tools to deal with. In this Research paper, I would be throwing light on the threat to our privacy, for which we have little or no legislation. The lack of such legislation is increasing this threat on the society, as time passes by.

Cyber World: A Whisper Network Of Harrassments?

Siddharth Kumar & Aniket Singh, B.A. LL.B (Hons.)
2nd Year Student, H.P. National Law University, Shimla.

Abstract

"Rather than shaming the woman for having her pictures splashed over revenge porn websites, people should extend their support and shame the criminal instead."

— Anangsha Alammyan

As the Internet becomes a significant part of human existence and a critical space for the voice of marginalized population to be acknowledged, a woman's inability to feel safe online is an impediment to her freedom and to her basic human rights. Yet the issue of online violence and harassment is often overlooked in discussions of violence against women. The problem is highly under-reported. The severity of violence is likely to be under-emphasized because the correlation between injuries sustained as a result of violence varies very little between severe and less severe instances of barbarity. It is a clear expression of gender discrimination and inequality that exists offline. Online, it simply amplifies. The first step to

addressing online violence against women is to recognize that it is a legitimate and harmful manifestation of gender-based violence. In India, like anywhere else, online violence and harassment of women and marginalized genders and sexualities is rampant, in contrast to Internet's initial premise of equal opportunity and neutrality. The epidemic of bullying has been another attention seeking problem in the internet. This can take the form of hacking, morphing of photographs, fake profiles on social networking sites or circulation of images without their consent – not from strangers alone but from those known to them. Or it can take the form of gendered hate mail, sexualized slurs, and uncomfortable references to body, nudity, sex life, and rape threats, which sometimes turn out to be explicit and graphic. Finally the authors will present a book review on a controversial book I Am a Troll: Inside the Secret World of the BJP's Digital Army which will help the readers to break the preconceived notions regarding the Cyber World and Cyber Crime.

KEYWORDS: - Cyber world, online, harassment, women, crime, social network.

Victimisation Of Women In The Internet Era: A Critical Study

Priyanka Dhar, Assistant Professor at Hidayatullah National Law University, Raipur
Anindhya Tiwari, Head of Department, School of Law, Mats University, Raipur

Abstract

Explicit content exploits young people and impacts women severely in many cases. The global access of internet though has opened flood gates of knowledge to people but it cannot be ignored that it has brought with itself series of serious concerns which governments globally are trying to tackle. Since people today have a very easy access to pornographic materials, the major issue that concerns the government is place restrictions in such a way that minors are prevented from having access to such adult content. The major discussion that take place are focused on the roles that parents, communities, technology and laws should play in order to protect children from cyberspace obscene and pornographic threats. But the impact of such cyberspace obscene and pornographic material has to be considered in a broader perspective with the impact it might have on the life of women who face abuse due to such content. Unfortunately the law makers and legislators hardly take cognizance of the matter even though there have been numerous researches available explaining the negative impact consumption of pornography by a spouse/partner in any household had on the physical and mental wellbeing of the other.

The paper offers an insight into how pornography and adult content victimizes women and the significant litigations and laws in various countries to prevent excessive consumption of pornography on the Internet.

Keywords: Pornography, Adult content, Internet, Cyber Pornography, Women, Victimization.

Proof and Forgery Of Electronic Record: New Challenges

Dr Veena Kumari, Assistant Professor,
University Institute of Legal studies, (H.P.U) Shimla-4

Abstract

The rapid growth of information and communication technologies over the last two decades has created revolution in both business transactions and individual practices. The world wide explosion of electronic commerce and development in the computer communication sectors are changing the delivery and availability of information and services. But the growth of

electronic media has also created new fields of criminality. Use of computers and internet has given origin to the crimes relating to electric records. Electronic forgery has created an eminent threat to the public and to world as a whole. Electronic forgery is committed generally by means of using electronic media and internet. Some of the common examples of electronic forgeries are Hacking, unauthorized access to someone's computer with intention of further committing further offences and digital information through the viruses, logic bombs etc. The electronic offences have been defined and made punishable under the Information Technologies Act; 2000.This Act has further amended some of the provisions of Indian Penal Code and Indian Evidence Act. But the predators of the electronic offences are generally more advanced than the law enforcing agencies. So in order to detect, prove and punish the offenders, the law enforcing Agencies must be made aware and technically advanced to implement these laws properly.

Cyber Crimes And Cyber Securities

Monika Shandil, Faculty Member, UILS, Shimla

Abstract

Human activities mostly depend on the technology. In the modern age internet is playing vital role in the development process of the society. Internet brought revolutionary changes in human life. It educates the masses and influences the thinking of people. Communication becomes very fast with the help of internet. People can easily access and transfer the information through internet. It provide a great opportunity in the field of communication on the other hand it become curse for the mankind where it is misused for the criminal activities. Cyber crimes become a challenge in today's digital world. It refers to the activities done with criminal purpose in cyberspace with the help of computers and internet. It includes cyber stalking, cyber harassment, gambling, hacking, cracking, virus etc. Cyber security is very important as it protect networks, devices, program and data from unauthorised accesses. This paper deals with cyber crimes, cyber securities like privacy.

Challenges in Cyber Forensics Investigation in India

Vijay Kumar, Ph.D. Research scholar,
Law Department, H.P.U. Shimla -5

Abstract

Cyber forensics deals with application of investigation and analysis techniques to gather and preserve evidence from a computer device in a method accepted by the court of Law. In modern digital world with the easy access of computer and internet facilities criminals have changed their *modus oprendi*. The aim of the cyber forensics is not only to recover the evidence but to oppose a criminal activity. Law enforcement agencies facing a new challenge dealing with cybercrime investigation. Criminal acts being committed and the evidence of these activities is recorded in electronic form and moreover in cybercrime investigation in India it lacks technical experts and technically trained police officers. As per NCRB report 2015-16 cybercrimes in India are continuously increasing because of ineffective investigation the percentage of solved cases is very low and almost 60.1% cases were pending during 2015-16 as per the NCRB 2015-16 report. In present paper researcher will discuss various challenges which are faced while handling cybercrime investigation and which unknowingly slows down both investigation and conviction. It is also needed to analyze the existing legal regime relating to use and admissibility of cyber forensics in crime investigation and trial.

Keywords: Cybercrimes, Cyber Forensics, Investigation.

Menace of Cyber Crimes in India: An Overview of Legal Issues, Prevention and Enforcement Strategies

Dr. Karuna Machhan, Assistant Professor ,
University Institute of Legal Studies, H P University, email:
karunamachhan@gmail.com

Abstract

The millennium has witnessed the rise of Information Age and knowledge society. Globally, electronic technology has been growing in a geometric progression. . A boundless, timeless and spaceless medium has emerged to environ the future business, known as Cyber Medium. Indian Laws on contract, Evidence, crime and to her aspects are quite old and are still accommodating the demand of new millennium. Thus, the law known as Information Technology Act has addressed the considerable extent the legal questions involving in adopting the cyber medium for communication, contract, commerce, jurisdiction, governance, crime etc. One of the very important aspects which is quite relevant now a days is Cyber Crime. Crime is not a new phenomenon. With the technological development, only the means by which criminals are able to commit crime has vastly changed in some respect. As technology advance, so does the ways in which the criminals are able to pull off their dreadful activities. Frankly speaking, the criminals can now commit crime more anonymously and at a very quick speed. Contrary to this, the technology has helped the law enforcement catch perpetrators. Countries firstly tried to book the cyber criminals under traditional criminal laws but soon the legal activity started gaining with the passage of time. Today we venture into the virtual world of cyber space where the privacy does not exist at all.

Thus, Cyber crime has made a significant impact on the criminal justice system prevalent throughout the world. The effects are seen even more as nationals are constantly trying to provide faster and well organized services to the citizens. Cyber crime is the new challenge for the Indian society, industry and the law enforcement and the entire criminal justice system as a whole. The present trend shows that cyber crimes are likely to grow in extent and complexity as more and more people are accessing internet services for their various purposes. This paper is an attempt to highlight various cyber crimes which are emerging with the passage of time. One of the greatest loophole in the field of cyber crime is the absence of comprehensive law anywhere in the world. The issue of cyber crimes is further aggravated due to disproportional growth rate of internet and cyber law. An attempt has been made to highlight global legal trend towards cyber crimes, legal implications of the internet, preventive and enforcement strategies to control cyber crime etc.

Relationship Between Internet Right And Internet Security

Junesh Thakur, LLB **(H.P. University)**

Abstract

As we move into the 21th century communication, organizational functioning, scientific and industrial progress and technological innovation have paved the way for us to experience new and wonderful convenience. 2003 WORLD SUMMIT INFORMATION SOCIETY (WSIS) was convened under the auspice of UNITED NATIONS. After long they negotiations

between governments businesses and civil society representative the WSIS Declaration of principles was adopted reaffirming the importance of the information society to maintaining strengthen the human rights .Right to internet access and enjoy the right to freedom to expression and opinion and other fundamental human rights. Recent changes in technology arising from the convergence of communication and computing the truly breath taking and have already had a significant impact on may aspect of life .Crime such as organized crimes ,software ,video ,audio piracy are also being used co-ordinates and winding their activities even beyond National boundaries.

Project focuses on 4 major areas of security issues on the internet. Personal computer security relates useful information to the average surface at home .Organizations that support or oppose internet security measure hacking into cyber space Psychological approach.

The Impact of Cybercrimes on Art

Dr. Anjana Bhardwaj , Associate Professor in Painting
J.L.N.Govt. College of Fine Arts, Shimla

Abstract

The primary objective of a cybercrime is to steal money and this is the type of activity that the art world is most affected by. The modern technology is helping this new breed of criminals known as Cybercriminals that are making money from works of art without ever taking possession of any of it. The kind of fraud most common in this filed is the type in which the cyber criminals hack into an art dealer's e-mail account and after keeping a close eye on the correspondence between the gallery and its clients. When the gallery sends an invoice to a client through e-mail after a purchase, the conversation is intercepted by the hackers. They act as the gallery and send a fake invoice from the same gallery e-mail address to the client with a message asking them to ignore the first invoice and wire the payment to the account shown in the forged document.

Once the transfer of money is completed to the criminals' account, the hackers just disappear from the scene to avoid detection. With millions made in a single transaction it is always a comfortable choice for them. The same technique is used to hijack payments made by galleries to their artists too. Once the hackers gain access to the gallery's email contacts, they spread their wings easily, with fake-mails coming from some known source.The art market is a vulnerable place to such scams, this market is a very lucrative option for the hackers as art dealers and their clients often wire millions even after a single conversation. These fraudsters have already looted the likes of London gallery owners, Simon Lee, Laura Bartlett and Thomas Dane, as well as the giants in the art market like Swiss gallery Houser and Wirth. Losses in these cases are believed to have reached the hundreds of thousands of dollars.

Key words: art galleries, cybercrime, emails, invoice, market.

E-Banking Frauds and Risk Management

Anjali Bhardwaj

Abstract

Internet banking fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and transfer money to an account in a different bank. Internet banking fraud is a form of identity theft and is usually made possible through techniques such as phishing, lottery fraud scam, forgery etc.

Now internet banking is widely used to check account details, make purchase, pay bills, transfer funds, print statement etc. Generally the user identity is the customer identity number and password is provided to secure transactions. But due to some ignorance and silly mistakes customers can easily fall into the trap of internet scam or fraud done by skimming, hacking etc. The paper is focused to study and highlight the types and many ways of internet banking frauds that takes place in our banking system nowadays and also to understand and study the way of fraud risk management on the part of every individual bank fraud.

Competition Analysis In A Digitalized Economy

Anupriya Shyam, Graduated with B.A.LLB(Hons)
UILS, Panjab University, 2019.

Abstract

Without big data analytics, digital companies are blind and deaf, wandering out onto the web like a deer on a freeway. Data is the life and soul of the digital economy, garnering immense benefits for the companies as well as the users. However, this robust weapon is a potential distorter of the healthy competition in the market. The digital economy is peculiar, characterized by data enabled 'network effects' and 'contestability' and the incumbent competition policy fails to cater to the peculiar nature of this economy. The traditional method of competition analysis, which focuses on price competition and market share, falls short of addressing the anti-competitive conduct of the digital market, which rely on innovation and big data. The modus operandi of the digital market involves amassing massive user data based on their behavior on various online portals like Google search, amazon, Uber, Facebook etc. and then using that for targeted advertising which is the major source of revenue for these firms. Profits are not extracted from the users, rather relying on differentiated services, more and more users are kept hooked to the digital platform. A company with massive users and huge databases acquires a very strong position in the market, which enables it to behave anti-competitively in the market. Mergers and acquisitions in the digital arena further facilitate the acquisition of more data and escape the scrutiny of the competition regulators as presently combinations are evaluated based on turnovers, which criteria these digital markets do not fulfill. Secondly, while assessing the abuse of dominance by these entities, the pre-requisite of being dominant in the relevant market is seldom fulfilled. This is because of the faulty interpretation of the relevant market qua the digital companies, where the entire country is taken as the relevant geographical market, whereas internet penetration in an area should be a factor in deciding the relevant geographical market. As for the relevant product market, it has to be seen as to whether the abuse is in the digital market only in both the online and offline markets. This will greatly change the way the dominance of an enterprise and its abusive practices like predatory pricing is evaluated; as well as the evaluation of combinations. Another competition concern raised is pricing algorithms facilitated collusion, which are hard to establish and there are no regulations in place governing the use of pricing algorithms. The antidote to talking these issues is introducing, inter alia, 'data' as a factor while assessing any anti-competitive conduct of an entity.

Recent Trends In Protecting Intellectual Property Through Cyber Laws: Indian Perspective

CS Yogesh Sharma

Intellectual Property refers to category of law relating to the rights of the possessor of intangible products of innovation or ingenuity. Intellectual Property law awards special rights to definite owners of artistic works, technical inventions, and symbols or designs. Cyber law relatively a new field refers to the cluster of legal issues occurring with the exercise of communications technologies that create cyberspace or the Internet. These issues include intellectual property (primarily copyright and trademarks), privacy, free speech and the suitable exercise of jurisdiction and authority over transactions and communications in cyberspace. It covers criminal and civil issues ranging from financial crimes to cyber bullying to First and Fourth Amendment rights.

The introduction of Information Technology and computers in India has created a new world in the cyberspace leading to various legal challenges and at times solutions. Copyrights, trademarks, designs, layout and circuit designs in the current digital environment, are interwoven with the electronic technology therefore more affirmative protective laws are required to guard new inventions and creations and also to save the real owners from economic losses.

Therefore to understand the various legal systems that may govern this area it is essential to have knowledge of not only cyber laws and Intellectual Property Laws but also of Conflicts of Law and international law. Though diverse approaches and legislations have been enacted by the Government for delivering a secure configuration against cyber threats, however it is the duty of the owner of intellectual property right to invalidate and reduce mala fide acts of criminals by taking proactive measures. This paper explicates various issues associated with the protection of Intellectual Property through Cyber Laws in Indian.

Keywords: Cyber law, Intellectual Property, Information Technology, Computers.

Cyber Security Laws And Policies In India And of Other Countries

Ishani Kanwar
3rd Sem., B.A.LL.B. (Hons)
HPUILS

Cyber security is the state or process of protecting and recovering networks, devices, and programs from any type of cyber attack. Cyber attacks are an evolving danger to organizations, employees, and consumers. They may be designed to access or destroy sensitive data or extort money. The state of 'cyber terrorism' has proliferated in the recent time when the cyber threat started developing to a great extent. However, with such attacks several attacks laws have also been developed with first importance being given to the IT ACT,2000. It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the **UNCITRAL Model** Law on International Commercial Arbitration recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

Several countries across the world have passed various laws to protect the cyber world from any attacks. Some examples-

Cyber Crimes in India: Issues and Challenges

Dr. Sandeep Kumar,
Assistant Prof. H.P. University Institute of Legal Studies,
Ava Lodge, Chaura Maidan, Shimla (H.P)

Abstract

Cyber-crimes have become a common phenomenon in India. Very often personal data of individuals' is required by various agencies and organisations dealing with public on different capacities. Once data is supplied, individuals do not have any control over supplied data which has aggravated the problem of cyber security. In India, various laws exist to protect personal data and privacy of the individual but poor implementation of those laws and unawareness about possible cyber-crimes associated with misuse of the data has made those laws virtually ineffective. Having this background in mind, the present study aims to examine data protection laws in India to ascertain the loopholes in them. The study will also offer some suggestions to prevent misuse of personal data and cyber-crimes in India. The study is purely theoretical in nature. It is based on secondary data which has been taken from articles, journals, websites, magazines and law books.

Key Words:- Cyber, Crimes, Data, Privacy, Protection.