INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

HARASSMENT AGAINST WOMEN IN INDIA: A CRITICAL LOOK AT THE LEGAL FRAMEWORK AND VICTIM PROTECTION MECHANISMS

AUTHORED BY - MALIK SAIMABEE ANSAR AHMAD
BALLB (2nd Year), Kes Shri Jayantilal. H. Patil Law College.

Abstract

Cyber harassment of Indian women is one of the serious problems, and it is growing at an appalling rate in the cyber world. Due to the increasing use of the internet and online platforms, cybercrimes are taking new shapes, which do not Favour women in any part of society. This paper is a critical examination of what cybercrimes committed against women entail, the extent and impact of such crimes in India, particularly in relation to the legal system as well as the enforcement regime in place to combat these crimes.

Such types of cybercrimes are most often perpetrated against women, including online harassment, cyberstalking, revenge pornography, identity theft, and non-consensual sale of intimate images. Online space anonymity and accessibility are likely to contribute to these crimes. The situation has been worsened by the fact that sophisticated technologies such as deep fake morphing, i.e., have, in the past few years, been abused to create sexualized and manipulated content at the detriment of women. These actions carry severe psychological, emotional, and reputational harm on the victims.

Even after legal provisions about Bharatiya Nyaya Samhita, 2023[1] (India).Information Technology Act, 2000 (India).Indian Penal Code, 1860 (India), the enforcement remains low. Cyber harassment has many cases, which go unreported due to lack of legal reedier measures, stigma of the subject matter, and lack of confidence in the law-enforcing agencies. In addition, insufficient training, technology expertise, and time delays in the process are disadvantages to the success of investigation and prosecution.

The cybercrime trend is dynamic and shifting whereby the victims of cybercrimes are various

[1] Bharatiya Nyaya Sanhita, 2023. (2023). *Government of India.* https://www.indiacode.nic.in

ISSN: 2582-6433

groups, although to different extents. However, women continue to be particularly vulnerable to internet harassment and sexual crimes on social networks. Those who fall prey to such crimes are women belonging to any socio-economic background; hence, cyber harassment is not simply a legal issue but also a serious social problem.

This paper indicates the gaps in the current legal framework and emphasizes the idea that it needs to be more authoritative, the authorities should be more effective, the mechanisms of victim protection should be more robust, and people should be more informed about digital matters. In order to eliminate cyber harassment of women, a thorough, victim-sensitive, and technologically receptive legal approach should be established so as to ensure justice and security for women in cyberspace.

Keywords: Cyber Crime, Women, Cyber Harassment, IT Act

Introduction

Cyberspace has been formed as part of modern life. During the time of rapid technological growth of electronic technologies and access to the internet, human beings rely on the internet as a means of communication, place of employment, education, business, and socialization. The Internet has rendered the world a global village whereby individuals can exchange ideas, give their views, and participate in social, political, and economic undertakings without geographical limits. The social network applications such as Facebook, and Instagram, all other dating app, have given the digital communication where individuals can interact freely, market, and create groups.

However, there are also some overwhelming difficulties in the development of cyberspace among all of these beneficial processes. It is the same features that enable free expression, such as anonymity, speediness, and global accessibility, that have made the internet a haven of cybercrime. One of the most concerning aspects of cybercrime is its tendency to target women. In India, where the existing social order tends to suggest the disparities on the gender premises, the virtual realm has unfortunately replicated and, in the majority of cases, worsened the disparities.

The victims of cyber harassment against women in India are taking place in numerous forms, including cyberstalking, online abuse, gender-based trolling through publishing personal

ISSN: 2582-6433

photographs without permission, defamation, and publishing of personal photographs without permission. The ability to perpetrate crimes with the help of digital tools (anonymously towards the victim) is the power of the perpetrator and complicates the identification and subsequent legal action against the perpetrator. Smartphones, accessibility to the internet, and the absence of robust implementation mechanisms have helped to push the rate of cybercrimes committed against women high, which is alarming. As indicated by the statistics released by the National Crime Records Bureau (NCRB), online harassment as well as stalking and other cybercrimes perpetrated against women have steadily been on the increase in the past few years.

The IT Act of 2000 [2]is the best law in India that governs offenses related to cybercrime, and thus it forms the foundation upon which cybercrime is handled. The Indian Penal Code also applies in regard to the online offense to a certain extent. However, despite such laws, there are no appropriate legal remedies for women victims of cyber harassment. Such intertwining of problems as the lack of gender-specific protection, the need to adhere to jurisdiction, the lack of digital education among the employees of law enforcement agencies, and the delay in the courts affect the effectiveness of these legal frameworks.

Thus, since the internet continues to be a powerful tool of empowerment, activism, and inclusive development, there also exist new and emergent forms of digital violence against women. What is therefore urgently needed is not only the need to strengthen the legal system but also to ensure easier implementation and protection measures based on victim targeting to tackle cyber harassment of women in India.

Types of cybercrime that result in digital victimization

In India, cyber-harassment of women takes various forms, and this is because cybercrime is diverse in digital times. As social networking sites have evolved at a very high rate and with the rising presence of individual profiles on the internet, cyberspace has become a place of empowerment and weakness in women. The internet offers perpetrators anonymity, convenient accessibility, and speed with which they are able to commit different types of digital abuse. Cyberbullying, cyberstalking, hacking, and phishing are the common forms of cybercrime all over the world. Yet, under a closer analysis in the specific case of women, such crimes are usually gendered and targeted. Abuse of social networking sites like Facebook, Instagram, and

[2] Information Technology Act, 2000. (2000). *Government of India.* https://www.meity.gov.in

ISSN: 2582-6433

Twitter has also helped to cause an increase in crimes like trolling, cloning of fake profiles, morphing images, cyber defamation, and cyber abuse. These are crimes that do not only intrude on privacy but also destroy dignity, reputation, and psychological well-being.

The crimes against women in cyberspace may be classified into the following broad categories:
Cyberstalking
"Cyberstalking" refers to the internet or use of digital gadgets to stalk, spy on, or bully a woman. The offender can send threatening or unwanted messages, stalk the activity of the victim carefully on the Internet, or even seek to infiltrate her personal life. This chronic behaviour has frequently caused psychological traumas, fear, anxiety, and disturbance of life routines.

Online Harassment
Online harassment involves verbal abuse, threats, sexually explicit messages, and defamation of women by means of online platforms. Misogynistic remarks and character assassination as usually performed by men are common phenomena. Victim-blaming in most instances disheartens reporting and upholds social stigma.

Cyber Pornography and Non-Consensual Publication of Privatized Material

Unauthorized publication or distribution of intimate images or videos is one of the most severe types of cyber harassment. This comprises so-called revenge pornography, involving the distribution of private materials without permission to embarrass or extort the victim. This issue is further enhanced by image morphing and deepfake technology, which changes photographs digitally to form materials that are sexually explicit. This leads to extreme distress and loneliness, damaged reputation, and, in certain instances, extortion.

Cyberbullying and Trolling

Cyberbullying entails instances of frequent insulting actions in a bid to harass or humiliate the female gender through the Internet. Trolling, especially, consists of publishing inflammatory or offensive messages in order to attract emotional responses. When it is directed at females, it is often sexist, misogynistic, or even sexually abusive. Female personalities in the open arena, including journalists, activists, and politicians, are highly vulnerable to such organized attacks.

ISSN: 2582-6433

The increased rate of the existing cyber harassment types proves the idea that cybercrime against women is not only a technological problem but also a social and gendered one.

Overview to Cyber Crimes against Women

Cyber harassment against women in India is most common in the form of online harassment. It is the abuse of digital platforms to send abusive, threatening, defamatory, and offensive content to women. This can be done via social media platforms, messaging applications, or email, among other online forums. According to studies by the National Commission for Women, a high percentage of women have undergone some type of online abuse. Such events can cause serious psychological outcomes such as anxiety, emotional stress, fear, and a feeling of continuous insecurity. Therefore, lots of females are not safe and insecure on the Internet.

The problem of online abuse has become international, and people of any age can be the users of this type of internet. But gender-based bullying, trolling, stalking, body shaming, and character assassination are specifically aimed at women. Anonymity and expansive coverage of the internet only serve to empower the wrongdoers and to complicate the pursuit and responsibility of the latter.

In response to the increasing risk of cybercrimes, India has passed the Information Technology Act, 2000, to combat cybercrimes and control the activities of the digital world. The Act categorizes the several cyber offenses and outlines punishment for criminal online behaviours. Besides the IT Act, there are other provisions in the criminal law that are applied to instances of online harassment and abuse. Even with all these legal measures in place, there are still issues with the enforcement, awareness, and the effective protection of victims.

The rise in cases of cyber harassment of women is a strong indication that there is a dire need to enforce laws more, implement gender-sensitive policing policies, offer digital literacy programs, and create easy-to-use complaint systems to create safer online spaces for women in India.

Cybercrime Laws in India

The high rate of cybercrimes perpetrated against women in India has forced the state to reinforce its legal provisions in fighting cybercrimes. Due to the growth of internet connectivity

ISSN: 2582-6433

and the internet, internet-related crimes such as online harassment, identity theft, cyberstalking, and sharing of intimate images have increased. As a reaction to this, India has come up with a mixture of statutory provisions under both criminal law and civil law in order to provide safeguards and responsibility. The main legal tools that regulate cyber offenses are the Information Technology Act, 2000; the Indian Penal Code; and the Protection of Women against Domestic Violence Act, 2005.

The overall Indian legislation on cybercrime is the Information Technology Act, 2000 (IT Act). First passed as a law to give electronic transactions and digital signatures legal recognition, the Act has also provided offenses and penalties concerning cyber misconduct.

The IT act criminalizes the following activities:
Breaking and entry to computer systems.
Personation and identity theft.
Online fraud
Electronic stalking
Obscene content: publication or distribution of obscene content.
The act imparts authority to prosecute cyber offenses and gives fines and imprisonment depending on the seriousness of the offense. It also helps in the creation of cybercrime cells in the different states to be able to enforce it effectively.
The Information Technology (Amendment) Act, 2008, was the further addition of new scopes of cybercrimes and added penalties, more especially those related to cyber terrorism, data breaches, and online exploitation.
Indian Penal Code (IPC)[3]
In India, the criminal law is still based on the Indian Penal Code of 1860. Though it was initially signed many years earlier, before the digital age, it has been interpreted and modified to support cybercrimes against females.
Under IPC there are relevant provisions that include
Section 354A - Sexual harassment
Section 354C - Voyeurism
Stalking (including cyberstalking) is found in section 354D.
Section 499 - Defamation

[3] Indian Penal Code, 1860. (1860). *Government of India*. https://www.indiacode.nic.in

ISSN: 2582-6433

Section 509 - the degradation of the woman of honour.

The IPC punishes direct offenders as well as those that abet them. Courts have also used the judicial interpretation to apply case-old criminal law to the online misconduct, which has to ace sure digital avenues are not used to provide safe havens to the perpetrators.

Protection of Women against Domestic Violence Act, 2005.[45]

The Protection of Women from Domestic Violence Act, 2005 (PWDVA) is a civil law that is mainly designed to protect women against domestic violence. The Act takes a comprehensive definition of domestic violence, which includes

1. Physical abuse
2. Sexual abuse
3. Emotional and verbal abuse
4. Economic abuse

The Act does not specifically address the issue of cybercrime, but the online harassment in domestic relationships (including Internet threats, spying, and the transmission of personal information) can be discussed in its context. The PWDVA gives protection orders and residence orders as well as monetary relief and other civil remedy

Regulatory & Institutional Measures

Besides the statutory laws, the regulatory bodies are also relevant in the fight against cyber threats. The Reserve Bank of India has also put up outlines to protect online banking and internet transactions to avoid monetary fraud and electronic misuse.

Moreover, the agencies and cells of cybercrime conduct investigations at both the central and state tiers to respond to complaints and punish offenders.

Difficulties related to combating cybercrimes against women.

A low rate of reporting is one of the greatest challenges in fighting the cybercrimes against women. Many victims do not go to law enforcement agencies because of fear of being discriminated against or stigmatized or because their reputations are at risk or because they are

[4] Protection of Women from Domestic Violence Act, 2005. (2005). *Government of India.* https://www.indiacode.nic.in

[5] Protection of Women from Domestic Violence Act, 2005. (2005). *Government of India.* https://www.indiacode.nic.in

ISSN: 2582-6433

expected to be harassed further. Women, in most instances, are not aware of their rights in the law, or they do not know about the available means of reporting and solutions.

The other critical issue is of a legal and institutional nature. Despite having the statutory provisions in the Indian Penal Code and the Information Technology Act, 2000, the working provisions are often challenged. The enforcement agencies might not have the technical skills, infrastructure, or even training to effectively pursue digital crimes. Moreover, the fact that the cyber laws have ambiguities and inconsistencies in their interpretation may bring different cases into the court with different results. Such delays in the justice system not only undermine justice but also serve as a deterrent to popular confidence in the legal system.

Thus, although India does have a formal law system to combat cybercrimes against women, there remain the problems of underreporting, lack of enforcement, and the issue of inconsistency in interpretation that impedes its efficacy.

Government Initiatives and Policies

The Government of India has put in place a number of policy measures and institutional mechanisms to deal with the increasing cases of cyber-crimes against women and children. The Cyber Crime Prevention against Women and Children (CCPWC) Scheme, which was introduced by the Ministry of Home Affairs in 2018, is one of those initiatives.[6]

The CCPWC Scheme will enable the enhancement of the effectiveness of the states and union territories in addressing cyber offenses against women and children. Financial aid under this scheme is to set up special cybercrime police stations and cybercrime cells. It also promotes the development of specialized cyber forensic labs within every state and union territory in order to boost efficiency in the investigations and enhance the best collection and preservation of digital evidence.

The initiative is aimed at enhancing digital infrastructure and access to technology in addition to the enhancement of enforcement mechanisms. The government would ensure that it narrows the digital divide by improving the quality and access to digital services to facilitate safer access to technology, especially among women.

[6] National Crime Records Bureau. (2023). *Crime in India 2022: Statistics on cybercrimes.* Ministry of Home Affairs. https://ncrb.gov.in

ISSN: 2582-6433

Moreover, the government has indicated that it is looking forward to having industrial corridors and smart cities with high technological infrastructure. These projects will be developed to include the current high-speed and modern communication systems and integrated logistics. It is also suggested to upgrade and modernize existing infrastructure in industrial clusters. These advancements will result in an enhancement of technology, enhanced connectivity, and a more comfortable and efficient online environment.

The application of technology against cybercrimes

Despite the revolution that technological change has brought to the modern life and the connection that has led to a higher rate of connectivity, it has also ensured that cybercriminals have more access to exploiting vulnerable individuals particularly ladies. Even the digital tools themselves, which are employed when communicating and sharing information, could be misused to harass and steal identities, stalk, and exploit individuals online. However, technology is not a source of risk only but it is also an effective source in preventing, detecting and responding to cybercrimes. One of the most crucial changes that occurred in this field is the use of AI and ML is growing fast in world of cybercrimes. The AI systems have the ability to scan the internet space in real-time and detect potential infractions. After processing a big amount of data, AI algorithms are capable of identifying the abnormal pattern of behaviour and filter out potentially malicious content and inform the authorities or administrators of the sites that something wrong has been done and needs to be done. This aggressive approach will make it possible to act in time and reduce the risks of damages. Machine learning models are also quite useful in behavioural anomaly detection. These systems are also trained and can be able to identify abnormalities that may define a fraudulent or abusive activity. The AI-powered tools are also popular in the applications of phishing detection, automated content moderation, and cyber threat intelligence. In addition, automated incident response systems provide companies with an opportunity to restrain and respond to attacks before they can cause significant damage. Encryption technologies are also a way of guaranteeing cybersecurity since information that is sensitive is not exposed to the wrong hands. Personal information, financial transactions, and personal messages are greatly encrypted and this reduces the risk of identity theft as well as data leakage. Other important tools in the investigation of cybercrimes are the digital forensic tools since they enable the collection, preservation, and analysis of electronic evidence. Altogether, the technological developments offer many layers of protection networks that reduce the areas of vulnerability, enhance cyberspace security, and enable law enforcement bodies to combat cyber-crimes against women. Therefore, it is evident that technology has been

ISSN: 2582-6433

provided clearly to help propel cybercrimes, yet it is the most appropriate to deter and manage crimes in the digital age.

Best Practices of preventing women cyber crimes

This increasing number of cases of cybercrimes experienced by women in India is an indicator that more preventive awareness and digital safety habits are required. Despite the legal escape, the first, and the best line of defence against online harassment and stalking, identity theft and exploitation is personal precaution. The following best practices may go a long way of reducing most of the victimization probability. Individual Prevention Interventions. Strong and Unique Passwords One of the most straightforward yet effective ways of cybersecurity awareness entail the use of hard passwords. The passwords should have 12 characters and they should include mixed case letters, numbers and special characters. The information that can be guessed with ease such as names, date of birth or common phrases have to be avoided. The secret is also enhanced through the use of various accounts which are secured using different passwords. Multi-Factor Authentication and Two-Factor Authentication. The Multi-Factor Authentication or Two-Factor Authentication (2FA) enables an additional layer of security because it requires a second authentication process such as a one-time code sent to a phone. This reduces significantly any possibilities of unauthorized access even in case of hacked passwords. Privacy and Social Media Consciousness. Social media sites are supposed to be highly secured regarding privacy. The profiles should be set to private and personal information should not be revealed such as phone numbers, addresses and personal photos. Some kind of care should be observed by any user before accepting a friend request or a stranger since cyber criminals usually target their victims using spoofed profiles. Confidentiality of Sensitive Material. The spreading of intimate photographs or personal data on the internet is highly dangerous of blackmail and so-called sextortion. No sensitive data should be stored in the devices which are automatically connected to the cloud solutions without encryption. It is even possible to retrieve lost files. Secure Shopping and Payments. The public Wi-Fi networks should not be used to execute financial transactions or any communication that is confidential. Users are thus advised to type the address of the websites in browsers rather than using doubtful links in order to minimize their chances of exposing themselves to phishing attacks. Antivirus Protection and Software Update. Continuous updating of the operating system, applications and the antivirus software ensure that the security vulnerabilities that have been identified are tackled. The antivirus software available in the market today can be installed by reputable antivirus vendors and it is capable of identifying and preventing such malicious software before they can get

ISSN: 2582-6433

access to personal data. Device and Hardware Safety Webcams are to be covered with physical covering in case they are not utilized to prevent unauthorized surveillance. The data that belongs to a person must be permanently destroyed to avoid misuse prior to repairing, selling or disposing electronic products. Mechanism of institutional and Legal support. Where the preventive measures are not effective to the victims, the victims can seek institutional and legal remedies. Official Reporting Portal In case of cybercrimes, the complaints can be diverted at the National Cyber Crime Reporting Portal that exclusively deals with women and child crimes. Helpline Services The national cybercrime helpline number can be called 1930 or women helpline number can be called 1091 and immediate assistance can be requested. Legal Provisions Protection of victims may be done through the use of the Information Technology Act, 2000, particularly the following: Invasion of privacy - Section 66E. o Publishing or publishing obscene material. A Publishing sexually-explicit material: 67A. There are also specifications provided in the Bharatiya Nyaya Sanhita that regulate the crimes such as stalking and the acts which are directed to insulting the modesty of a woman. Evidence Preservation The victim is highly encouraged to store screenshots, chat records, emails among other electronic evidences. Destruction of ill-intended materials may compromise a lawsuit; therefore, digital evidence would be required in order to carry out an investigation. It was also possible to empower women greatly to feel safe in the digital space through participating in workshops and awareness campaigns.

Conclusion

One of the most important problems of the digital age is Indian women and Cyber Harassment. Though the technological advancement has created a tremendous opportunity in the field of communication, empowerment and socio-economic inclusion, it has presented new avenues of gender-based violence on the Internet. The number of cyberstalking, Internet harassment, and non-consensual transmission of intimate images, phishing, and Internet defamation is on the increase, and that is why a new and efficient legal tool is very much desired. Another legal framework that India has gained to deal with cybercrimes is under the Information Technology Act, 2000, the criminal law applicable, and the Bharatiya Nyaya Sanhita, 2023. The national programs such as Cyber Crime Prevention against Women and Children (CCPWC) Scheme and the National Cyber Crime Reporting Portal are also among the institutional responses that demonstrate that the government has been keen on the mechanisms of improving the enforcement. However, despite these endeavours, there exist massive loopholes in the effective application, network of victim, technical expertise and timely research. The underreporting of

ISSN: 2582-6433

cybercrimes due to fear, stigma, ignorance, and the low degree of trust in the authorities is one of the problems. The current laws are further compromised by the deterrent effect which has been compromised by the time lapse in the procedures and a rather complex nature of jurisdiction and disparity in interpreting the law. In short to enjoy equality, dignity, and justice in the contemporary society, it is vital to ensure that women are accorded safe inclusive digital space. The struggle against Cyber Harassment and safeguarding the rights of women in the rapidly evolving digitization era of the Indian fast changing world requires a technologically progressive, legally adequate, and socially conscious government.

References

Information Technology Act, 2000. (2000). *Government of India.* https://www.meity.gov.in

Bharatiya Nyaya Samhita, 2023. (2023). *Government of India.* https://www.indiacode.nic.in

Indian Penal Code, 1860. (1860). *Government of India.* https://www.indiacode.nic.in

Protection of Women from Domestic Violence Act, 2005. (2005). *Government of India.* https://www.indiacode.nic.in

National Crime Records Bureau. (2023). *Crime in India 2022: Statistics on cyber crimes.* Ministry of Home Affairs. https://ncrb.gov.in

Ministry of Home Affairs. (2018). *Cyber Crime Prevention against Women and Children (CCPWC) Scheme.* Government of India. https://www.mha.gov.in

National Commission for Women. (2022). *Report on cyber crimes against women.* https://ncw.nic.in

Wall, D. S. (2017). *Cybercrime: The transformation of crime in the information age.* Polity Press.

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the victimization of women: Laws, rights and regulations.* IGI Global.

Jaishankar, K. (Ed.). (2011). *Cyber criminology: Exploring internet crimes and criminal behavior.* CRC Press.

Kshetri, N. (2010). *The global cybercrime industry: Economic, institutional and strategic perspectives.* Springer.