LEEWAY IN THE DIGITAL SPACE: RISE OF CYBER CRIME, A CASE STUDY

Abstract

Nation's governance policy of digital politics has marked an era of rise of internet and digital space. All the information gathered in the e-governance platform has made information accessible with just a tap or a click on a digital device. This information ranges from personal to political. Such system's policy, therefore, emphasises the possibility of information technology in the governance. Rise if IT in the policy making and its execution is the administrative criteria of the time. On the hindsight, the evolution of digital world overall, has also provided a leeway for the rise of cyber-crime in the digital space. Pornography, human trafficking and murder are some of the dark Hidden Services. People, commonly, become the victim of phishing. The study on such leeway in the digital space of digital politics resonates the concept of digital divide. The term 'digital divide' here is used to express a gap between internet users. There is a gap between digital device users and internet users. These look similar but a basic difference between them lies in a gap of knowledge of the internet and its usage in the world of the web. The ration between these two remains lopsided. Every society is threatened by the dangers of cyber-crimes usually conducted through the deep web and the dark web. The paper, here, attempts to explore a rise of new culture of crime in the digital space. And to narrow down the study, the case study will focus an impact of cyber-crime in the region of Siliguri. The objectives are to find the nature of cyber-crime, impact of phishing in our area of exploration and to study digital divide of the region. Our data collections are through interviews, questionnaire and official judicial website.

Keywords: Digital space, cyber-crime, threat, digital divide, new culture

Authors

Bedika Rai
Assistant Professor
Department of English
Kalipada Ghosh Tarai Mahavidyala
bedika.rai@gmail.com

Dr. Basudeo Thapa
Assistant Professor
Department of Nepali
Kalipada Ghosh Tarai Mahavidyala
mikham390@gmail.com

I. INTRODUCTION

Digital space usually refers to a platform used through digital device for several e-services. Gathering of information in such a space, lead to accessibility of information both personal and political. Information Technology has marked a new era of governance. Major concern today, of most of the countries, in digital space has become Data protection. Data security is an utmost essential condition for the security of the nation overall. It is accessible through various outsourcing agencies. BPOs play an important role in the dissemination of information. Such companies are a threat to nation's security and individual's right to digital space. The very digital space therefore, provides a leeway for dark hidden services or simply said cyber-crimes. National Security Presidential Directives 54 / Homeland Security Presidential Directives 23 defines cyber-space as, 'the interdependent network of information technology infrastructures, and include the Internet, telecommunications networks, and embedded processors and controllers in critical industries.' (*Cyberspace, Cybersecurity and Cybercrime* 47)

Crime through digital space has become rampant. It is easily executed without leaving much of a trace for common man. Internet's role is vital in e-services. It can be simply understood as computer network or links used to communicate. Internet is defined as 'an electronic communications network that connects computer networks and organizational facilities around the world' (Webster). Internet users vary from social media surfer like Google or Twitter, to program creators like Java to e-service providers like Swiggy. Dark web and Deep web are a part of world wide web. Moore and Rid, in 2015, reported of 2,723 active dark web sites. According to *Cyber-attack Public International Law of Cyberspace,* "Cyber-attack basically aims at either preventing access to a network by overwhelming it or taking it offline or gaining entry into computer networks to monitor activities and extract information on the system or on user's system…"(pg 154).

Dark web is a part of the internet that remains hidden in search engines and is accessible by way of software which allows users and website operators to remain hidden. Similarly, Deep web can be understood as anything that remains hidden or isn't accessible through search engine like Google. It includes password-protected or encrypted networks. Dark web can be functional in places and spaces where free speech is in danger and internet isn't made available or isn't permissible. Mostly, political issues or sensitive issues from all sphere of life, without freedom of expression, uses dark web to express their issues and condition. On a hindsight, it is used as an instrument to commit cyber-crimes too. Cyber-crime can be understood in two broader ways- cyber-dependent crimes and cyber-enabled crimes. 'Cyber Strategy Guidebook' defines cyber-dependent crimes "offences that can only be committed using a computer, computer-networks or other form of information communications technology" (*Cyber Strategy Guidebook* 10). This includes hacking attacks using viruses and other malwares. On the other hand, cyber-enabled crimes are understood as crimes committed by using computers, internet networks and many other types of ICT. This however, can be committed without ICT also. Fraud and theft are the most common cyber-enabled crime.

Cyber-crime, therefore, in general, can be defined as any crime that involves the knowledge of technology, which is communicated or executed through digital devices such as computer. Cyber-crime is associated with network, computer, and internet. It is often

termed as "Computer crime, Network crime, High-Tech crime, Internet crime, Online crime, and Information age crime" (*Combating Cyber Crime* 2). Such crime involves target, use of tools and evidences for execution by the attackers and for investigation by the investigators. Some common techniques and tools used to execute cyber-crimes are as follows-

- Malware- it means a program is inserted into a system to gather information.
- Phishing- it means a use of spoof emails or fake websites through weblinks to deceive people into personal financial details.
- Spoofing- it means a deceiving text from attacker which is made to look authentic such as links from Banks.
- Spyware- it refers to a kind of a malware installed secretly to gather information both personal and public.
- Trojan- it refers to an application that appears reliable which controls the victim's computer system.

Cyber-crime evidences are the most challenging ones. All courts have their respective condition in accepting or moreover in recognizing authentic evidences. Text files, audio-videos, images are some of the evidences that requires thorough authentic examination to be liable to become evidence. Proper study of government's policies to combat such crimes will be helpful. It helps in awareness about such crimes. More, it provides information about laws and legal procedure to file complaints against cyber-crimes.

Cyber-crime and Cyber-labs in India are an interesting area of study. The rise of digital space and the use of internet in digital devices often do not correspond to one another. This digital divide can be one of the major causes of its rise. It becomes difficult to govern or control such rise. New culture of digital crimes or web crimes has affected both capitalist countries like USA and developing countries like India. India's policies of governance within and outside aspires her to stand as a powerful rising nation in Asia. This digital divide in India is strikingly visible too. Difference between rural India and growing cities, generation with knowledge of digital world and generation that programs digital services, and online user communities and offline user communities is marked social and economic differences. In such a digital gap, cyber-crime in India rises easily and fast. To control the crime, amendment of Indian Penal Code and Indian Evidence Act was done. And instead emphasized on cyber-crimes and valued digital evidences. India follows a standard operating procedure for investigation of such crimes.

On the hindsight of Cyber-crime mention in *Cyber Crime Investigation Manual* 9, "Information technology and the Internet have led to innovation and economic growth, but have also created new avenues for malicious actors to perpetuate crimes". NCRB reported rise of cyber-crime in India by 47.5% in 2018-20. They also reported four major types of cyber-crimes in India. They are-

- Hacking of computer system
- Forgery
- Pornography
- Frauds

The rise of cyber-crimes in India from 2018 – 2020 can be viewed in the following figure:

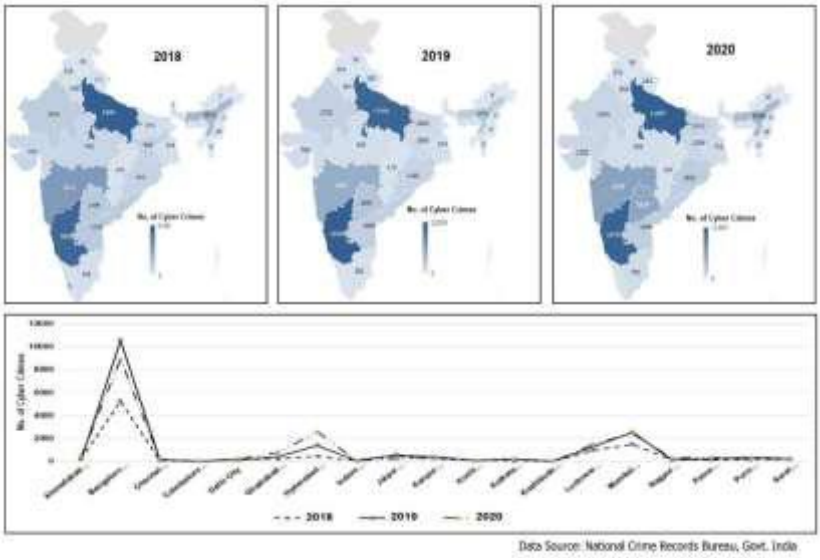

Figure 1: Rise of cyber-crimes in India from 2018 – 2020

To investigate, Central Bureau of Investigation plays a vital role. First Cyber-crime police station was established in Bangalore. Today, every state in India has cyber-crime cells to handle such cases. National Association of Software and Service Companies (NASSCOM), attempts to promote development to country's security. They train Information technology department and police officers in handling cases of cyber-crime. Cyber Labs Programs are organised by NASSCOM. Their main focus is to-

- Establish more cyber labs for speedy investigation
- Provide cyber-crime preventive trainings to police as well as other agencies
- Provide standardize investigation methods and tools
- Suggest legal measures for prevention of cyber-crimes

Mumbai, Thane, Pune and Bangalore are the first four cities in India where cyber labs were conducted. Data Security Council of India (DSCI) later established cyber labs in other cities such as in Chennai, Hyderabad and Haryana. Proper investigation leading to the arrest of the convicts can take the case to its ultimate state. Punishment of committing cyber-crimes in India is 3 years of imprisonment with fine of 5 lakhs. Law and order have been made possible for the victims to rise from such attacks/ theft. National Crime Records Bureau (NCRB) records the rise of cyber-crime only in Kolkata as 32 cases in 2018 to 160 in 2019 and 172 in 2020 as cited from ncrb.gov.in.

II. METHODOLOGY

The study here aims at finding cases of cyber-crime in the region and the nature of it. Methodology for our study used is quantitative. Data has been collected through random sampling and pilot survey. Interview and questionnaire was prepared as a part of the survey. The respondents were Ms. Rangu Souriya, founder of Kanchanjunga Uddhar Kendra, Siliguri, West Bengal, Mr. Rajkumar Tamang, social worker Kanchanjunga Uddhar Kendra, Bagdogra, West Bengal, and Mr. Raju Nepali, founder of Duars Express, Odlabari, Duars.

These two NGOs cover cyber-crime cases of North Bengal, Northeast and Sikkim region. The questionnaire for the participants consists of:

- How often do you get cases related to cyber-crime?
- What age group and literacy rate group are being affected by it?
- How often are you informed about cyber related crimes in comparison to other forms of crimes?
- Do you take into consideration all the informed cases?
- What measures do you apply to those cases for solution or rescuing of the victims?
- What kind of affects and influences of cyber-crimes can be found among families and society?
- To what degree are the families and society aware about cyber-crimes in today's time?
- What do you think is the role of digital space in the rise of cyber-space?
- Comparatively, has digital space caused more problems or provided protection against such crimes?
- Are the predators of cyber-crime mostly from the region or outside one's region or state?

Secondary data has been collected from official judicial website, online newsreports,Data Collection from Crime Branch Siliguri and NGO Kanchenjunga UddarKendra, Siliguri and Duars Express.

III. CASE STUDY

The case study shall now narrow into its area of research. Our area of study is Siliguri. Siliguri is a rising city in the northern part of West Bengal. It lies in the Himalayan foothills. The city is surrounded by tea gardens. It is also a transit center as it connects with neighbouring lands Nepal, Bangladesh and Bhutan and neighbouring states Assam and Odisha. Interstate and International nature of the city makes it a centre of economic growth in the northern part of West Bengal. It thus, becomes a city of easy infiltration as well.

We began with our study of Cyber Crime cases filed and reported in Siliguri region. We applied simple random sampling. Out of total of first one hundred FIR of the year 2022, cyber-crime cases under IPC sections 419/420, 66C IT ACT, 379/420, 384, 354C/ 66E/67 IT ACT, 506/509, 499/500, 406, and 465/468/471 were commonly found as follows:

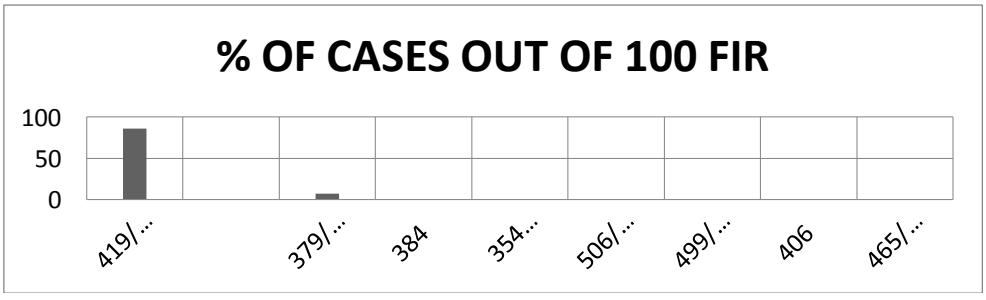

Figure 2: Cyber Crime cases filed and reported in Siliguri region

The participant responded to the role of social media as the main cause of easy execution of cyber-crimes by citing some cases from the investigation. The participant's response was that quite often they get cyber-crime related cases as digital space has become a common ground of meeting people. Messenger, Facebook, WhatsApp was regarded as some of the common digital space through which predators hunt for money through blackmails. The participant views that 'The online marketing or networking sites have led to easy data transfer system which is used by predators for their benefit'. By hacking information from digital space, they demand money usually by blackmailing the victims.

The participant referred to a recent case of Pankhabari region. A victim there, having failed to give away the demanded money, was blackmailed by circulating her nude photos randomly to her contact list. Such cases abound in large number. Major target group are aged 16 and above. Teenagers and college students who appear to be tech-savvy but do not realise consequences of misuse of digital space and digital device are the main victims. NGOs are approached by the victim or their well-wishers who seek solution to such problems. Mostly, unaware of the law-and-order policies, for help they also approach NGOs. Victims mostly are teenagers but are not the only ones. Married women have been victims of cyber-crime.

Victims go through suicidal attempts, depressive impact and psychological trauma. Social workers help them out of such situation through counselling and laboured rescue field works. The participant opined strongly that rise of smart phones and availability of internet has lately increased cases of cyber-crime. 2019 onward such cases have boomed to another level. To prevent from falling a prey, they organise awareness programmes regarding proper use of digital devices and the networks, legal procedures of cases and inform about contact points that can help solve a case.

Further counselling acts a major role in addressing victim's trauma. The participant stated that all victims look for solution in the first place. Cases of physical abuse through digital space has become a common crime case. Victims are lured into love relation scenario, whereby, in the name of love they are asked to exchange their photos and videos. Later predators use the very photos and videos as a tool to blackmail demanding ransom in return. Usually, such photos are edited into nude pictures and used as a threating tool. In such cases, victims go through severe psychological depression and look for immediate way out. Mostly, through counselling they encourage victims to face legal procedures against the predators for justice.

Counselling do not limit only to the victims. They attempt to counsel families and society of the victim as well. Acceptance by the families release victims from feeling ashamed or guilt-ridden. Awareness program for youth, adults, parents are also organised. To prevent from becoming a cyber-crime victim and to recover from the cyber-attack, Jon R. Hansen, suggests to become 'a member of organizations that work in prevention of cyber-crimes' and to 'work with local communities that support cyber-crime preventions effort' (*Cyber Crime Prevention* 282). A case from Pokhriabong is referred here by the participant. A married woman came in contact with a man who promised of love and sexually abused her. The predator recorded the activity and used it to blackmail her. The victim reported of stealing money from the family to pay the predator as demanded. Further she sold her gold jewellery to fulfil his demands. Lastly having no choice attempted suicide but was rescued.

Principal
Kalipada Ghosh Tarai Mahavidyalaya
PRINCIPAL
Kalipada Ghosh Tarai
Mahavidyalaya
Bagdogra

In most of the cases, parents remain unaware about cyber-crime. Ignorance of the public about awareness programs and their interest on more entertainment programs in the online platform has resulted in the failure of 100% impact of awareness programme. People's attention usually comes only after a crime has been committed instead of gathering up during prevention phase. She regards the ignorance or a decision to remain ignorant about misuse of digital space by the majority of people as a challenge in controlling the rise of cyber-crimes.

The participant holds a strong view about a necessity of having a digital space for the progress of a nation. But there lies a condition. If the space is used for right purpose with right measures, it can develop a nation faster. On the other hand, if used for wrong purpose, it can cause chaos to our socio-economic and political existence. There should have been an age limit to the use of both digital device and networking facilities to prevent children from falling prey to the hawk-like predators. Early exposure to the digital space, device and networking sites has led to early exposure of children to many more ways of gathering information as well as to evil norms and acts. Solution is not found in the digital space for those who are not tech-savvy or is unaware of dark hidden space used for maltreatments.

Those hackers or attackers have been found to be from other states like Rajasthan, Mumbai, Bangalore and Punjab as per their case related area. The participant refers to a case of Punjab-Pakistan border. The victim last tracked was in the Punjab-Pakistan border exactly four years back. The victim was lured into love relationship through a social media. On the request of the victim's family a search team did the investigation but with no success. The case remains unsolved. Types of cyber-crimes in which predators attack through online space as found in investigation cases are –

Table 1: Types of cyber-crimes

SL. NO	Types of Cyber Crime Reported	Age Group	Gender
1	Foreign friendship	20-40s	F
2	Import tax	20-30s	F
3	Threat through AV Media	15-30s	F
4	Sexual Abuse & Threats	16-30s	F
5	Lottery	20 -40	F&M
6	Bank related links	20-50	F&M

To the query regarding how the predators select or identify their victims, the participant states that they go for random selection by sending links, texts, friend requests or any other approaches. The one who often easily responds and keeps the communication becomes the victim. She cites a case that happened recently in Messenger. A gang of 600 members circulated nude pictures and videos of two minor in the group. The case was reported from Mirik. Priest from the church to which one of the minors belonged to approached the NGO for help after one of the victims attempted suicide. On enquiry as to how their nude pictures and videos went to the predator, they reported of having sent those by themselves after they were promised of love and were asked to do so for love. Later they were blackmailed and demanded money. Having failed to provide money, their pictures and videos were circulated openly in the digital space. Having said so, the search points out to

that category of people who seek love, attention and demand care but are left unaddressed to be more liable to become easy prey.

Siliguri being a city of economic exploration and border zone in the international security part, NGO also reports receiving such cases mostly from Nepal and the North-East. The other participant refers to a case of the North-East. The victim was brought to Matigara, Siliguri by one of her relatives to provide her job in a parlour. In reality, this minor was kept by a family consisting of husband, wife and a brother-in-law. They earned 5000 per hour by giving her to various clients. No body could doubt the family as they would stay in one colony not more than six months. A messenger from Sikkim asked for help. After several attempts for five years, she was tracked and the predators was arrested. The report says that the victim was forced into sex business while she was a minor of age 16. And by the time she was rescued she was 21. However, her family in Tura denied to take her back. In cases as such, ED gives full support to the NGO in rescuing the victims of human trafficking organised both in an online and offline method.

When the victims are rescued many time predators remain untracked because they use the same digital space to block all their information. The participant reports of one particular case from Pulbazar, Darjeeling, 2021 where a predator was arrested and the case is being legally handled in the court at present.

Lack of support from the family or loved ones or excessive facility given by the family leads to disbalance communication within family structure. Difference between duty and luxury and an ignorant attitude toward it also contributes to miscommunication or no communication in a family set-up. The participant believes that a balance between one's professional and personal life can prevent one from becoming a victim of cyber-crime. Exposure of the world through digital space, availability of advance digital devices and facility of internet networking sites also provides a space in the leeway of the digital world run through digital space, for predators to easily execute their plans in easy money-making process. More awareness regarding abuse of digital space needs to be made available to the public.

The other respondents informed that during the lockdown period maximum cases of cyber-crime was reported. Social media platform such as Instagram, Facebook and WhatsApp are the common platforms that the predators use. Most of the cases recorded are Bagdogra, Panitanki, Sikkim, and the tea garden areas. Educated class of young people are the ones to be easily liable to becoming prey. However, both married and unmarried, men and women have been the victims. He further informed that most of the victims belong to 13-40 years of age and all gendered people become the victims through such online platforms.

Digital space being used for various purposes such as online games, fantasy world, and groups like cannibalism has been a leeway to the usage of digital space. They report, around 30% of the population of Siliguri region remain aware of the darker side of internet and networking. Mr. Gurung shares a case that of the 16 years old from Naxalbari who was a victim of child marriage. Sexual abuse in one of the commonly executed crime through cyber-space around the world. There are all kinds of crimes such as drug peddling, trafficking, child marriage, child labour and smuggling that happens on a daily networking process in the Indo-Nepal border. They report that in 2017 there was more than 250 cyber-

crime cases reported from Bagdogra Airport. Awakening awareness should be spread through orientation programmes regarding cyber-crimes in academic institutions, administration level, family and among the youths.

IV. CONCLUSION

Our study of cyber-crime in Siliguri region, led to the exposure to regions nearby as well. Most of the cyber-crime cases reported are fraud, blackmailing, sexual abuse, threat and trafficking. Most of the fraud cases reported are links shared from reliable sources. These links shared either are bank links or lottery. Phishing is also the common fraud that FIR cases on cyber-crime in Siliguri states. Blackmailing is mostly found to occur through online friendship in our study. The craze for foreign friendship and personal attention leading to sharing of intimate photos and videos resulted in blackmailing the victims. Sexual abuse through online audios and videos is also rampantly found among the minors. Social media is also the site of exploitation for cyber-crime predators. They use the platform to share the intimate images randomly. Threatening the victims then becomes easy for the predators for easy money making. The very online friendship has also been reported to be an easy process of trafficking.

Victims are mostly of female gender. Though teenagers are in majority the victims, nevertheless, any age group flexible or available online all the time are liable to be victims. Many can be rescued if the case is shared and reported in the proper center such as Crime Branch and NGOs at the earliest. FIR of cyber-crime victims should be handled immediately as a procedure to trace and find the predators.

Counselling to the victims has been discovered to be helpful as a preventive method. It can help the victims regain prestige, confidence, and mental stability preventing them from self-harm such as suicide. Counselling of the families and society at large can help in accepting victims in normal way and in prevention of becoming a victim. Lack of communication within a family set-up can make people look for attention elsewhere giving opportunity to predators hunting randomly. One must be careful about the use of digital space and devices. Knowledge of both visible and hidden services of the digital space and using it for productivity, national security, and public progress can be beneficial. Many remain or choose to remain ignorant of cyber-crime. Many do not report the cases of cyber-crime at all. Many do not know procedure of fighting against cyber-crime. Awareness and information about cyber-labs, crime-branch should be made available to public or public should avail that information for prevention.

Cyber-crime is on the rise and world organisations have called conventions for the prevention against it. In the General Convention of the United Nations, 2000, a resolution was passed that stated every States to ensure its laws and practices to abide by cyber-protection and also stated that the legal system should protect data information uploaded in computer systems ensuring cyber-protection. Similarly, the Council of Europe, the European Union, ASEAN, APEC, and G-8 States conventions suggests and states the significance of cyber security.

One cannot disagree to the increase of cyber-crimes of all kinds with all online facilities on the platter. Nor can one disagree to the misuse of digital space for various crimes,

Principal
Kalipada Ghosh Tarai Mahavidyalaya

both national level and individual level. More studies in this area can function as awareness practice. This study is a result of random sampling and pilot survey. More detailed study on cyber-crime is a necessity to understand the impact of digital space in the rise of new crime culture, commonly called the cyber-crime in the region of Siliguri. Detailed study can provide other variations to explore. Accordingly, prevention system on the individual and community level should be improved and made available to public. Further study and research in this area of study can be beneficial at large.

REFERENCES

[1] Clancy, Thomas K., *Combating Cyber Crime: Essential Tools and Effective Organizational Structures, A Guide for Policy Makers and Managers*, National Center for Justice and the Rule of Law, 2007, The University of Mississippi School of Law
[2] CRC Press, *Cyberspace and Cybersecurity*, Taylor and Francis, Ed. 2, 2018, New York
[3] *Cyber Crime: Investigation Manual*, Data Security Council of India, New Delhi, 2011
[4] Interpol, *National Cybercrime Strategy Guidebook*, JAIF, April 2021, Japan-ASEAN Corporation
[5] Jensen et.al., *Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics*, The Information Society, December, 2007, ISSN: 0197-2243
[6] Kittichaisaree, Kriangsak, *Public International Law of Cyberspace*, Law, Governance and Technology Series 32, 2017, Springer
[7] Kremling, Janine & Parker, Amanda M. Sharp, *Cyberspace, Cybersecurity and Cybercrime*, SAGE, 2018, Ed. 1, United States of America
[8] Moore, Daniel & Rid, Thomas, 2016, *Cryptopolitik and the Darknet*, Survival, 58:1, 7-38, DOI: 10.1080/00396338.2016.1142085
[9] Reyes, Anthony, *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors*, 2007, Syngress Publishing Inc., New York
[10] Sarshar, Mubashshir, *Cyber Crimes and Effectiveness of Laws in India to Control Them*, 2009, National Law University, Delhi
[11] Webster, Merriam, "Internet." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/Internet. Accessed 11 Nov. 2022.
[12] NCRB, https://ncrb.gov.in/en/crime-in-india-table. Accessed 6 Jan. 2023.
[13] https://siliguripc.wbpolice.gov.in/fir.Accessed 6 Jan. 2023