An Analysis of Laws Relating to Online Sexual Abuse in India

By Ranadip Bhattacharya

Research Scholar, WBNUJS, Kolkata

DOI: doi.org/10.55662/CYLR.2024.3101

Abstract

The internet has made massive inroads in our lives, personally as well as professionally. Therefore, it is only natural that crimes on the internet too will increase. This paper specifically focuses on sexual crimes on the internet and the legal and judicial treatment such crime receives. The paper will discuss the various kinds of sexual crimes that can happen online and will also discuss crimes that have yet to receive adequate judicial or legal attention. The paper will try to deduce what can be termed as 'sexually abusive' on the internet and the interface between the two since sexual conduct is inherently physical and the internet dispenses with physicality. The paper will also dwell on the limitations or difficulties in actually deducing a cybercrime since in many cases the distinction between the online and the offline world may get blurred. The paper will discuss the phenomenon of cyberrape has been contemplated in other jurisdictions notably Israel. The paper will further discuss the development of the law to this end in various jurisdictions including India and will also deal with the judicial treatment that has been meted out to various cybercrimes of a sexual nature in India. The paper will also discuss the current state of Indian laws about online sexual abuse, with specific reference to the various amendments in laws that have been affected concerning online sexual offences and also analyse the efficacy of such amendments. Thereafter the paper will discuss various case laws in India about sexual offences that have occurred online and the approach taken by the courts. Finally, the paper will end with an analysis of what are the changes that are needed in the law and how such changes may be brought about to ensure a meaningful development of the law.

Keywords: Cybercrime, Sexual Abuse, Cyberrape, Online Sexual Abuse, Information Technology Act, Crimes Against Women

Cyber Law Reporter
ISSN 2583 7060
Volume 3 Issue 1 – January - March 2024
This work is licensed under CC BY-SA 4.0.

Introduction

It needs no mention that the internet has revolutionized our lives in more ways than we can imagine or care to enumerate. From the simplest of stuff, such as communicating with our friends or colleagues, to somewhat more important issues such as consulting a doctor, the internet has made its presence felt everywhere. Arguably, the greatest revolution that the internet has ushered in, is in the area of communication. Communication has been made infinitely simpler and faster all thanks to information and communication technology. Collection and dissemination of ideas is now very easy and cheap owing to the easy availability of the internet. This stance has been bolstered by the COVID-19 pandemic which has increased our dependence on the internet manifold due to the consequent lockdown and the resultant restriction of our mobility. It may be said to be a foregone conclusion that the presence of the internet in our lives, and our concomitant dependence on it will just increase.

One area in which the internet is gradually making its presence felt to a greater degree is the area of sexual pleasure. 'Cybersex' may sound oxymoronic since sex is inherently a physical act and physical is dispensable in the cyber-realm. However, online sex is an actual and active phenomenon. Cooper et al have described cybersex as the use of the internet for sexual gratificationⁱⁱ. Juan Ramon Barrada and others have broadly categorized cybersex into two categories: solitary, such as watching pornography, or interactive such as indulging in sex chat or sextingⁱⁱⁱ. Whatever the mode, the essence is that the person getting involved in cybersex seeks sexual satisfaction.

The advantages of seeking sexual gratification on the internet are many. Apart from the fact that it is cheap and easily available, the Internet also offers a veneer of anonymity which makes it easier for people to seek sexual gratification online. The advent of a host of casual dating apps seems to just reinforce this fact. The internet has also been hailed as a massively empowering space wherein people from alternate sexualities can come together and share their thoughts while still protecting their identities. Journalist Samantha Cole has argued that sexual communication and groups formed an integral part of the internet from its halcyon days and had a telling effect on the identity, community, and consent with regard to sex by the information highway^{iv}.

This change has also been reflected in India. India Today in its 17th sex survey reports that Indians have become more open about their sexuality with a greater discard of inhibitions relating to sex and the report tries to bring about a correlation between the massive penetration of the internet and internet devices and such sexual openness^v. In a nutshell, it may be said that the internet is a potent tool for empowerment sexual and otherwise and an even more important means for giving voice to people of alternate sexualities who might otherwise continue to remain voiceless.

Sexual Abuse and The Internet

Similar to sexual intercourse, sexual abuse on the internet might also sound oxymoronic but sexual abuse, or sexual violence, on the internet is also an active reality. Online sexual abuse does not fall into a set definition; however, it includes a broad spectrum of activities that are unwelcome to the recipient of such activity and make such recipient feel unsafe. For this paper, online sexual abuse implies any online activity that makes the recipient of such activity:

- i. Feel uncomfortable; or
- ii. Unsafe while using the internet;

and

- i. Where such activity has a genesis in sex; or
- ii. The target of such abuse has been so chosen because of sex (gender); or
- iii. The concerned activity has a sexual angle.

The spectrum of such online behaviour is rather broad, they may stretch from unwanted sexual communication to blackmailing, sexually misusing someone else's picture to the extreme cases of revenge porn. More often than not the lines between online sexual abuse and offline sexual abuse may get blurred wherein sexual abuse may spill over from the online world to the real world or may lead to actual consequences in the physical world. Again, cases of pure online abuse may have consequences in the offline world as well like in case the victim of such abuse suffers psychological trauma similar to, and in some cases even greater than, the trauma suffered in cases of physical abuse.

An unwarranted breach of the sexual privacy of an internet user may also be termed as a case of cyber sexual abuse, specifically in cases where the user had a reasonable expectation of such privacy. Such breach may occur either through another user, specifically the one the victim was engaging with or it may also occur via a third party such as the intermediary or even

another person who might have intercepted such communication.

Statistics show that after the pandemic, cases of harassment of women, in general, have increased manifold^{vi} and cases of online harassment have increased fivefold^{vii}, thereby again leading to the victims of such harassment, women to be more precise, feeling unsafe on the internet. Such a scenario also has a tacit effect on the economic empowerment of women since many women use the Internet as a means of economic empowerment. One of the most important reasons for the feeling of heightened insecurity on the internet on the part of such victims is due to the comprehensive nature of the net, wherein the victim may have to relive their trauma over and over again, and escape is virtually impossible^{viii}. Even celebrities and women with privileged backgrounds are not immune from such attacks and the consequent trauma^{ix}.

A recent trend of online sexual abuse is deepfake which is nothing but digitally altering the face or body of a person to make them appear in fake situations^x. This is somewhat similar to the ubiquitous offence of morphing except that owing to the advancement of technology and improvements in Artificial Intelligence deepfakes can be very convincing and hard to detect. This is used as a potent tool for online sexual abuse.

Cyberrape

The issue of cyberrape was intimately discussed in the seminal article "A Rape in Cyberspace, or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society" by journalist Julian Dibbell^{xi}. This was one of the first mentions of the phenomenon of cyberrape which brought it into the focus. The situation described in this article had occurred completely online wherein a particular user of the online community Lambda MOO used his avatar, entitled Mr. Bungle, to commit actions, by the use of a subprogramme, which were attributed to other users. Mr. Bungle forced the other users to perform

Cyber Law Reporter
ISSN 2583 7060
Volume 3 Issue 1 – January - March 2024
This work is licensed under CC BY-SA 4.0.

sexual actions on themselves and on each other against the wishes of such users. This entire action was performed online through the use of technology, yet several of the victims of such actions felt violated in real life and had to face emotional trauma, with one user crying due to such trauma^{xii}. Many users termed the entire incident as a 'breach of civility'. There were no offline repercussions of the act; in the online realm, the avatar of Mr. Bungle was terminated by another user^{xiii}.

The above issue is relevant even today when the cyber world is being increasingly used for affecting sexual abuse and violence, and an increasing number of such harm also spills online. In 2011, Israel for the first time formally indicted a person for the offence of 'verbal rape' or 'communicative rape' in two cases. In the first case, a male person fraudulently misrepresented himself as a doctor to a minor and gave her instructions to penetrate herself. In the second case, a fifty-year-old male posed online as a teenage boy and induced a minor to penetrate herself. In both cases, the rape charges were dropped and were substituted by charges of aggravated indecent acts^{xiv}.

In another case in 2002, a housewife in New Jersey found all of her personal information posted online by one of her in-laws. The post not only contained her personal information but also described her physical features in detail and invited people to come and rape her^{xv}. The North Carolina governor had since then signed a law that made the usage of the internet to lure or entice someone into committing a crime, a crime in itself^{xvi}. The above scenario conforms to the modern notion of data rape wherein the personal information of a particular user is made public with nefarious, often sexual, ends. Martha McCaughey et al argue that information privacy violations that get used for sexual privacy violations are akin to the traditional notion of rape that gets extrapolated to the online realm^{xvii}. The UK police is also investigating the complaint of a minor girl who claims to have been raped in the metaverse in January 2024^{xviii}.

Rape is often a means to establish power as much as it is about sex, the internet, with its inherent anonymity and often makes people feel empowered enough to use the internet to commit gender and sexual crimes with a motive to show the victim of such crimes their place. The legal response to such motive should be to ensure a fair distribution and balance of power between all users of the net since the internet may be termed as egalitarian in the truest sense of the term.

Cyber Law Reporter ISSN 2583 7060

Response of the Law

The term cyber sexual abuse still eludes a precise definition and one of the greatest stumbling

blocks in deducing such a definition is the fact that the lines between online and offline abuse

often get blurred. Added to it is also the fact in cases where the entire activity is restricted

online, the police do not attribute much importance to such cases. This apathy is present even

though the trauma faced by the victim is real.

The Indian legislature has taken many positive steps in the direction of combating cyber sexual

abuse, such as amendment in the Indian Penal Code, expansion of the Prevention of Sexual

Harassment at Workplace Act, and suitable modification of the Information Technology Act.

For instance section 354A of the IPC makes showing pornography to a woman against her will

an offence, section 354C of the IPC makes voyeurism a punishable offence and criminalizes

the 'watching or capturing of a woman engaging in a private act without her permission or

consent'. Furthermore, even if such capturing were by consent, distributing such pictures

without the victim's consent is punishable. Section 354D criminalizes stalking a lady except

for reasonable and legal purposes. Section 509 makes the breach of privacy of a woman a

punishable offence.

Notably, the offences contemplated in the IPC are gynocentric wherein the victim can only be

a female.

The Information Technology Act too contemplates several sexual offences. For instance,

section 66C of the Act makes identity theft with fraudulent or dishonest methods a criminal

offence. 66D contemplates cheating by personation using computer resources, and section 66E

punishes the violation of privacy of an individual. Section 67 makes the publishing or

transmitting of lascivious material over electronic medium a punishable offence and section

67A prohibits transmitting or publishing sexually explicit act or conduct upon the internet.

Finally, section 67B punishes the searching, downloading, publishing or transmitting of child

pornography. Unlike the IPC, the IT Act is gender-neutral.

It is to be further noted that sections 66C, 66D and 66E can be reasonably expanded to included

sexual misdemeanors in their scope as well.

The Indecent Representation of Women Act prohibits producing, distributing or circulating any indecent representation of women in any form. Finally, the POSH Act was specifically designed to target harassment of women in the workplace and cyberspace is considered an extension of a woman's workplace if she were to use the internet for her work^{xix}. The government has also floated a National Cyber Crime Reporting Portal for ease of lodging of complaints about cybercrimes and increasing awareness about cybercrimes.

If one were to view the above provisions, it can be noticed that the sexual harassment laws are heavily tilted towards women. Statistically, this makes sense since women form an overwhelming majority of victims of sexual abuse including sexual abuse faced online. However, it may be argued that since the online world by its very nature dispenses with gender as a requirement, laws relating to online sexual abuse should be gender-neutral. The Information Technology Act conforms to this view. But the fact remains that women face a lot of online flak simply for their gender, irrespective of their social stance^{xx}. Not only women, but even people of alternate sexuality may find the online space to be rather unsafe, often such lack of safety spilling over to the offline world^{xxi}.

The Union Territories of Jammu and Kashmir and Ladakh specifically recognize and criminalize the offence of sextortion which has been defined as:

"(1) Whoever,--

- (a) being in a position of authority; or
- (b) being in a fiduciary relationship; or
- (c) being a public servant,

abuses such authority or fiduciary relationship or misuses his official position to employ physical or non physical forms of coercion to extort or demand sexual favours from any woman in exchange of some benefits or other favours that such person is empowered to grant or withhold, shall be guilty of offence of sextortion.

Explanation.--For the purpose of this section, sexual favour shall mean and include any kind of unwanted sexual activity ranging from sexually suggestive conduct, sexually explicit actions such as touching, exposure of private body parts to sexual intercourse, including exposure over the electronic mode of communication.^{xxii}"

The section also contemplates punishment for the crime to the tune of "rigorous imprisonment

which shall not be less than three years but may extend to five years and also with fine".

There are many areas in the law which could well be done with a relook or an overhaul,

specifically in cases of sexual offences committed online. For instance, in terms of identity

theft, as discussed in the case of Iraq, if a person were to misrepresent himself or herself to

induce another to indulge in some sexual act at the behest of the first person, which such other

person would not have otherwise indulged in, such an action should be specifically treated as

a cyber sexual crime.

Similar to the offence discussed in the New Jersey situation above, sharing personal details of

one person online to incite others to sexually abuse the first person should also be treated as a

substantive cyber sexual offence.

It may be noted that revenge porn as a crime does not find separate mention in the laws, but it

may read into several of the sections above notably 354C of the IPC and 67A of the IT Act.

Judicial Approach to Online Harassment

The number of cases of online sexual harassment is increasing in India. The year 2022

registered a rather steep growth in the number of such cases as compared to 2016 and 2017. Of

course, many people attribute the growth to not only an increase in crime but an increased

reporting of such crimes owing to the activity of the governmental machinery in reporting such

crimesxxiii.

The judicial approach to cases of online sexual approach too has been novel with the courts

often resorting to judicial novelty based on the facts of the case before them. In the case of

Majeesh K Mathew v State of Kerala^{xxiv}, the Kerala High Court specifically laid down that

making sexually explicit remarks against a woman on social media was tantamount to online

sexual harassment. In the year 2015, an additional Chief Metropolitan Magistrate's Court in

Maharashtra handed the state's first conviction in a cyber stalking case, wherein the accused

was charged and found guilty under sections 66E of the IT Act and 509 of the IPCxxv. This case

was unique in the sense that the entire action was conducted online, the guilty party had sent

obscene pictures to the aggrieved party via email. Ironically, the relationship between the

parties had initially started offline.

Courts in India have often had to deal with a question of balance between Article 19(1) of the

Constitution of India and internet safety. This can be illustrated by the case of Shirin RK v

State of Kerala^{xxvi} in which the High Court at Kerala specifically upheld the 'right to have

access to the internet becomes a part of right to education as well as right to privacy under

Article 21 of the Constitution of India'. Therefore, taking forward the analogy, it may be argued

that any action that makes it difficult for a person to access or use the internet is violative of

the Constitution as well.

Way Forward

In terms of technology, law typically tends to be responsive since the rate of flux of technology

is greater than the rate or speed of change in law. There have been cases wherein fresh crimes

have emerged only after the advent of, and the increased penetration of, the internet. Examples

would include phenomena such as cyberstalking, doxing, and catfishing.

Recently Justice Hima Kohli of the Supreme Court expressed her views and alarm on the

increasing use of technology and social media for sexually harassing others. She particularly

voiced her concerns about deepfake keeping in mind the convincing results deepfake

generates xxvii. This shows the extent to which technology has penetrated our lives, which

compels even top judges of the country to contemplate the same. In a sense this reflects a very

positive change as in the judiciary of our country is indeed keeping track of the times and is

open to adapting itself with the changes in society and economy.

The balance between technology, crime and the law is delicate at best and nebulous at worst.

Keeping in mind the Lessig Code^{xxviii}, we cannot, and should not, try to control technology.

Innovations such as deepfake have been possible only because of the recent and huge

advancement in technology. What the law can and should do is try to control the misuse of

technology for crimes. Of course, the Indian legislature as the judiciary has made good strides

in this matter, but more needs to be done. Maneka Gandhi, then the Union Minister for Woman

and Child Development had once commented that the cyber laws in India are too weak to any

concrete action against online sexual abusers^{xxix}. Sadly, there does not seem to have been much progress made from that. Of course, there have been changes in the cyber laws in the country, there has been the IT Amendment Rules, 2023, but they were mostly like imposing censorship upon the content of what can be and what cannot be carried by various web portals, a control on gaming and increased responsibility upon intermediaries including prevention of incitement of sexual offences^{xxx}. The Digital Data Protection Act, 2023 also does not any direction in this regard.

Suggestions And Conclusion

The first step that the law can take is to ensure a proper and clear definition of what constitutes online sexual abuse. such a definition may be based on a categorization of activities that may be abusive, or based on consequences to such activities that may follow or a combination of both these factors. The second step is that the laws relating to such abuse in online spaces should be strictly gender-neutral, especially because many people of alternate sexuality find the internet a good place to air their voices. The third step is that there should be proper sensitization to all stakeholders concerning the impact of sexual abuse in the online space. The current apathy towards such abuse must be legally and administratively tackled. Conviction rates of cybercrimes in India are currently very low, mainly due to such apathy coupled with ignorance^{xxxi}. This is all the more relevant with a greater shift towards online administrative functions. The provision of sextortion should be made applicable nationally. The offence of revenge porn should be given more teeth and it should be treated as a kind of cyber rape. The act of sharing without consent intimate videos of people should be treated as a separate and serious sexual offence irrespective of gender and irrespective of the motive of the person sharing. In general, sexual abuse laws pertaining to the internet should be given more recognition and teeth.

The courts have already played an active role in recognizing sexual abuse on the internet. With social media forming a parallel society comprising various individual courts too should view sexual abuse more comprehensively, trying to extrapolate and expand the existing norms of sexual abuse in the physical world to the online world as well. Ultimately the users of the information highway too should be more proactive and aware. They should not take the cloak

Cyber Law Reporter
ISSN 2583 7060
Volume 3 Issue 1 – January - March 2024
This work is licensed under CC BY-SA 4.0.

of anonymity offered by the internet as a convenient pass to indulge in nefarious activities. It must be borne in mind that the internet makes us powerful, but with such power comes great responsibility as well. Misusing such responsibility can and should lead to legal consequences.

References

xiii Ibid

ⁱ Kumar, S., Gupta, G. and Singh, K.R. (2015) '5G: Revolution of future communication technology', 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) [Preprint]. doi:10.1109/icgciot.2015.7380446.

ii COOPER, A. et al. (2004) 'Online sexual activity: An Examination of Potentially Problematic Behaviors', Sexual Addiction & Sexual Addiction & Compulsivity, 11(3), pp. 129–143. doi:10.1080/10720160490882642.

iii Barrada, J.R. et al. (2019) 'Not all online sexual activities are the same', Frontiers in Psychology, 10. doi:10.3389/fpsyg.2019.00339.

^{iv} Brandom, R. (2022) A history of the horny side of the internet, The Verge. Available at: https://www.theverge.com/2022/10/23/23415019/samantha-cole-interview-how-sex-changed-the-internet-bbs-porn-kink (Accessed: 14 December 2023).

^v Sex survey 2019: Virginity important for 53%, majority against filming sex (2022) India Today. Available at: https://www.indiatoday.in/lifestyle/story/the-more-things-change-1614722-2019-11-01 (Accessed: 14 January 2024).

vi Prakash, V. (2021) 'Covid-19-impact: Increased violence against women in India', *Kardan Journal of Social Sciences and Humanities*, 4(1), pp. 57–67. doi:10.31841/kjssh.2021.5.

vii The Indian Express (2021) 'After Covid, cases of online harassment spiked by 5 times', 7 January, p. 3.

viii Hubbard, L. and Keighley, R. (2023) 'LGBTIQ hate, harassment, and abuse online', *Queer Victimology*, pp. 37–49. doi:10.4324/9781003400981-5.

ix Chakraborty, S. (2021) 'Not just men, there are women trolls too: Sreelekha lashes o .. Read more at: http://timesofindia.indiatimes.com/articleshow/84710033.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst', *Times of India*, 25 July. Available at: https://timesofindia.indiatimes.com/entertainment/bengali/movies/news/not-just-men-there-are-women-trolls-too-sreelekha-lashes-out/articleshow/84710033.cms?from=mdr (Accessed: 15 August 2021).

^x Barney, N. and Wigmore, I. (2023) *What is Deepfake Ai? A definition from TechTarget*, *WhatIs*. Available at: https://www.techtarget.com/whatis/definition/deepfake (Accessed: 14 January 2024).

xi Eisinger, D. (2017) *The original internet abuse story: Julian Dibbell 20 years after 'a rape in cyberspace'*, *The Daily Beast*. Available at: https://www.thedailybeast.com/the-original-internet-abuse-story-julian-dibbell-20-years-after-a-rape-in-cyberspace (Accessed: 14 January 2024).

xii Buck, S. (2017) *The 'rape in cyber space' from 25 years ago posed problems we still haven't solved today*, *Medium*. Available at: https://timeline.com/rape-in-cyberspace-lambdamoo-da9cf0c74e9e (Accessed: 14 January 2024).

- xiv Harduf, A. (2021) 'Rape Goes Cyber: Online Violations of Sexual Autonomy', *University of Baltimore Law Review*, 50(3), pp. 357–397.
- xv Hopkins, K. (2005) Computer Crime Research Center, 'Cyber-rape' outlawed: N.J. cracks down on computer-aided crime. Available at: https://www.crime-research.org/news/19.01.2005/910/ (Accessed: 14 December 2023).
- xvi Common Computer Crime Statutes (2006).
- xvii McCaughey, M. and Cermele, J. (2022) 'Violations of sexual and information privacy: Understanding Dataraid in a (cyber)rape culture', *Violence Against Women*, 28(15–16), pp. 3955–3976. doi:10.1177/10778012211070316.
- xviii Sales, N.J. (2024) 'A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future?', *The Guardian*, 5 January. Available at: https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta (Accessed: 08 January 2024).
- xix Sanjeev Mishra v. Disciplinary Authority and General Manager, Bank of Baroda and Ors, S.B. Civil Writ Petition No.150/2021
- xx Sawhney, A. (2022) *Cybercrime against women up 28% since 2019, Karnataka's share highest: NCRB*, *Business Standard*. Available at: https://www.business-standard.com/article/current-affairs/cybercrime-against-women-up-28-since-2019-national-crime-records-bureau-122083001139_1.html (Accessed: 14 January 2024).
- xxi Banerjee, A. (2023) 'Surge in Cybercrimes: NCRB Data Highlights Concerns for Queer Community', *The Mooknayak*, 7 December. Available at: https://en.themooknayak.com/lgbtq-news/surge-in-cybercrimes-ncrb-data-highlights-concerns-for-queer-community (Accessed: 10 January 2024).
- xxii Jammu and Kashmir Reorganization (Adaptation of Central Laws) Order, 2020, (2020).
- $^{\rm xxiii}$ Basuroy, T. (2023) India: Number of cyber crimes related to sexual harassment 2022, Statista. Available at: https://www.statista.com/statistics/875912/india-number-of-cyber-crimes-related-to-sexual-harassment/#:~:text=Number%20of%20cyber%20crimes%20related%20to%20sexual%20harassment%20India%202016%2D2022&text=There%20were%20over%203.4%20thousand,the%20year%202016%20and%202017 . (Accessed: 14 January 2024).
- xxiv Majeesh K.Mathew v. State of Kerala and Another, B.A. No.3833 of 2018
- xxv The State (Cyber Cell) Complainant v. Yogesh Pandurang Prabhu r/o. Vashi Accused, C.C. NO. 3700686/PS/2009
- xxvi FaheemaShirin R.K.v. State of Kerala & Others, WP(C).No.19716 OF 2019(L).
- xxvii www.ETLegalWorld.com (2023) *SC judge Voices concern over online harassment, says Deepfake Tech raises privacy invasion alarms ET legalworld, ETLegalWorld.com.* Available at: https://legal.economictimes.indiatimes.com/news/litigation/sc-judge-voices-concern-over-online-harassment-says-deepfake-tech-raises-privacy-invasion-alarms/105872768 (Accessed: 10 January 2024).
- xxviii Lessig, L. (2000) Code and other laws of Cyberspace. New York: Basic Books.
- xxix The Indian Express (2016) 'Maneka Gandhi takes on cyber trolls, asks women victims to inform her', 6 July. Available at: https://indianexpress.com/article/india/india-news-india/maneka-gandhi-takes-on-cyber-trolls-asks-women-victims-to-inform-her-2896042/ (Accessed: 10 January 2020).
- xxx The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (2023).
- xxxi Chatterjee, A. (2022) 'Why are cybercrime convictions low in India? "Weak forensics, dark net & cross-border attacks", *The Print*, 21 December. Available at: https://theprint.in/tech/why-are-cybercrime-convictions-low-in-india-weak-forensics-dark-net-cross-border-attacks/1273191/ (Accessed: 21 December 2023).