
LEGAL DISCOURSE ON RIGHT TO BODILY AUTONOMY: LESSONS AND BEST PRACTICES

Dr. Mononita Kundu Das, St. Xavier's University Kolkata

Introduction:

Feminist concerns have found a place in law, increasingly over the past years. The 'digitalisation of intimacy' during the Covid-19 pandemic has caused an increase in overall sexual behaviour online, including an increase in sexual deviance online. Such digital sexual deviance includes online stalking, online sexual harassment, revenge pornography, online dating scams, etc. The typical victim of revenge pornography may very well be a man, or a transgender person. However, since the issue revolves around sexual autonomy and since the phenomenon has left most harrowing impacts on the lives of women, it cannot be studied without a feminist perspective.

Historical evidences:

The term 'revenge pornography' traces its origin back to the sensational case of American citizen, Hunter Moore, who hosted a blog on the internet and collected such intimate images from various sources and then disseminated it on his website without the consent of the people depicted in those images. He earned revenue through advertisements and merchandising. At the time, there were no specific crime titled 'revenge pornography'. Hunter Moore was convicted and ultimately sentenced for the offence of identity theft. However, the term 'revenge pornography' was used in this case for the first time. The phenomenon of nonconsensual dissemination of 'private sexual images' (PSI hereinafter) also became a part of the public discourse. Garcia and Aitchison, have argued that online public shaming (abbreviated by the authors as OPS) has been used as tool of moral policing, where the victim is shamed online with the purpose of 'disqualifying her/him from normal discourse'. They deem the act of online shaming and abuse to be a 'reputational punishment'.

Typologies of the Offence:

The phenomenon of 'revenge pornography' has been described by many authors in many different names. It has been called 'revenge pornography' 'non-consensual pornography', and

‘non-consensual sharing of intimate images’. The parameters of revenge pornography have not been well defined. Among the various prevalent term, Indian judiciary has only ever used term ‘sextortion’ to refer to image-based sexual abuse.

The offence of nonconsensual dissemination of PSIs or at least the offending act concerned must be well-defined. Ava Schein prefers the term ‘non-consensual pornography’ on the ground that not all dissemination is caused due to a revenge motive. Motive for dissemination or extortion under threat of dissemination can be varied and complex. The perpetrator might as well be disseminating the images for financial gain or mere notoriety. So, classifying the phenomenon as ‘revenge pornography’ may not be inclusive. As Samantha Bates puts it, “revenge porn is included under the umbrella of nonconsensual pornography, but nonconsensual pornography does not always include revenge porn”. In effect, the offending act can be the non-consensual capturing of PSIs and dissemination of the same; it can be consensual capturing of images and dissemination of the same; it can be capturing of images and threats of dissemination in connection to extortion; or any number of events involving the threat of dissemination.

An issue of difficulty vis-a-vis non-consensual pornography is that a large number of victims gave their consent to the recording or capturing of the image, which was later disseminated without their consent. Traditionally, there has been some indifference and even hostility to sexual autonomy of women. Women who have recorded intimate images themselves are often viewed as immoral or unworthy of protection. Often the existing social values end up putting responsibility on the victim for capturing intimate images of himself or herself. The victims who have captured their own PSIs are thought of as morally compromised.

The issue of ‘contextual privacy’ has not seeped deep enough into the public mind. In fact, all three of the major social networking sites, namely Facebook, YouTube and Twitter have no standard mechanism for ensuring human rights standard other than that of free speech. The use of ‘consent’ as an exception to criminal liability may be permissible in relatively trivial cases such as tattooing or boxing, but when resultant injury could be grave, consent should not act as an exception to criminal liability. Consent must be informed consent. The right to physical integrity or mental integrity should not be capable of being waived. In cases of non-consensual dissemination of PSIs, the mental integrity of the victim is injured through the effect of the dissemination itself and the resultant harassment that follows. Undoubtedly, consent to

capturing the image itself cannot be used as a defence for dissemination.

Of course, there is the larger issue of nonconsensual dissemination of images that has been morphed or edited. What Indian journalist Rana Ayub and American actress Scarlet Johanson have in common is that they have both been victimized by nonconsensual dissemination of fake intimate images online.

Among all the typologies of nonconsensual dissemination of intimate images, the images which are shared along with the personal contact details of the victims, have perhaps the most harrowing effect on the life and liberty of the victims. When the contact details and other personal information of the victims are shared along with the intimate photograph or video, it leads to ‘crowd sourcing’ of the harassment against them. The victim can suffer harassment and abuse from any unknown person on the internet who has incidentally stumbled upon the disseminated matter. It is in complete violation of the victim’s right to privacy and therefore, their right to life.

Consequences of Dissemination:

An in-depth study of 18 victims of nonconsensual dissemination of PSIs has revealed that victims experienced posttraumatic stress disorder (PTSD), suicidal thoughts, depression, anxiety, and other detrimental effects of their mental health, after their pornographic images were shared without their consent. Such dissemination hampers the victims’ right to reputation. *“While data are the economic language of digital culture, reputation is central to the cultural currency of networked and social media exchange.”*

Dissemination of intimate images or sexual images of private nature, without the consent of the people depicted in those images, is also an issue of privacy. Gautam Bhatia notes three traditions concerning ‘privacy’. The first one deals with privacy as a *‘spatial concept applicable to spaces.’* This would cover an individual’s right to not be subjected to monitoring at odd hours of night. The second concept *‘defends privacy in terms of relationships, communities or social institutions.’* The third concept *‘defines privacy in terms of an individual’s right to exercise her autonomy in the taking of private decisions about the use of her body.’* Non-consensual dissemination of intimate images violates the individual privacy by taking away the agency of the victim in publication of his or her intimate images.

In 'revenge pornography' for example, the victim has a right to exercise bodily autonomy and send any private intimate picture to a partner, without being exposed to the risk of publication of such images for the world to gawk. She has the right to keep such image private as against any person who is not the individual to whom she sent the image. In cases where victims were captured without their knowledge, such as in a changing room, he or she has the right to reasonably expect privacy while being engaged in an act of private nature.

Privacy is a right which is connected indistinguishably with individual dignity and personal liberty. In India, the scope of the right to 'life and personal liberty' has been widened with each passing judicial interpretation. Even so, unlike US right to liberty, which encompasses all freedoms that an individual ought to have, Indian concept of right to liberty is limited to 'personal liberty'. Indian Courts have already clarified that right to life is not '*mere animal existence*'. The meaning of 'personal liberty' too has been the subject matter of extensive debate. Even though Supreme Court initially refused to hold the right to privacy as a part of personal liberty in Kharak Singh's judgment, it later overruled itself in the landmark Puttaswamy judgment. Right to privacy includes the right to be forgotten. Victims of nonconsensual dissemination would be better off if this right is established in their favour.

Right to Privacy of Victims in USA

Internationally, the legislative reaction to non-consensual pornography has been slow. When the first few instances of revenge pornography happened in USA, the victims had only two recourses. First, they could opt for civil litigation under privacy violation tort, the relevant ones being 'intrusion upon seclusion' and 'public disclosure of a private fact'. Second, they could take action under copyright law, provided they themselves were the copyright owner. They had no direct remedy under criminal law.

The civil claims and tortious claims for protection of victims from non-consensual dissemination of PSIs were found ineffective. Possible reasons for their ineffectiveness were the victim's inability to pursue costly litigation, the failure of tort law to effectively take down the already disseminated images and the fact that the perpetrators may be insolvent or poor, rendering an action for damages toothless. Above all, most victims were primarily interested about removal of the disseminated images from the cyberspace.

Action to take-down the disseminated image proved to be difficult, as the cyberspace is not

merely a physical location. The victim could not simply demand that one single post be taken down. The concerned image could have been shared and re-shared exponentially across the cyberspace by the time the take-down notice was even considered. The ability to take down the shared content couldn't effectively be placed upon the perpetrator who originally disseminated the image. It had to be placed upon the 'intermediary'.

Section 230 of the Communications Decency Act (CDA) of USA grants intermediaries a certain level of protection from tortious liability of any third-party content. This section has made the take-down of disseminated PSIs from the internet even more difficult, due to the immunity it places on the intermediaries from third-party content. Under USA law, intermediaries often use this section to claim immunity for content published in the forum of the host intermediary. This section is a powerful safe harbour for intermediaries. In USA, websites such as Gawker, reportmyex.com were able to display intimate sexual videos of subjects without their consent due to the legal protection they enjoy under the Community Decency Act. Though such websites ought to have been regulated, a contrary argument against regulation was that regulations on publishing materials online would invariably curtail free-speech rights enjoyed by US citizens and also have an impact on news agencies. Moreover, taking away immunity of intermediaries would be economically devastating for the country as well.

Tortious liability was especially difficult to establish as only some American states like Texas recognised privacy tort laws, whereas other states like New York did not. Section 230 of the Community Decency Act, which is hailed a protection for free speech by those who support it, made it extremely difficult to make the offender as well as the intermediary liable for disseminated content under civil law. Holly Jacobs, who started the Cyber Civil Rights Initiative (CCRI) was herself a victim of revenge pornography. She had no recourse under criminal law when her intimate picture was shared across the web, along with her contact information. Since her experience, she has been fighting for criminalisation of revenge pornography.

Soon scholars Citron and Franks started to publicise the issue of revenge pornography by their scholarly pursuits and by bringing the issue into the zeitgeist. Over time, penal laws were enacted against revenge pornography. Yet the victims continued to face problems.

The U.S. Code: the Video Voyeurism Act has been criticised for its insufficiency in dealing with revenge pornography. The lack of a legislation ensuring the 'right to forget' in USA, unlike

in UK, caused a problem for victims. Victims barely have any recourse to bring down the disseminated images by 'de-listing' it. The advocacy initiative called the Cyber Civil Rights Initiative attempts to contact the websites on behalf of the victims, to get their intimate images de-listed. Yet victims are often left in the lurch.

When anti-revenge porn laws clashed with American first amendment rights, the Courts began to apply the principle of strict scrutiny to test the constitutionality of the criminal laws. New Jersey was the first state to criminalise revenge porn in 2014. Over the years, forty-three US states enacted their own revenge porn laws to stop the disclosure of PSIs of another. Most states make it a misdemeanour to violate the anti-dissemination laws. The crucial distinction between the state laws is that some states like California, Arkansas and Colorado, have introduced a criterion for malice or *mens rea* in the statute, whereas others have not.

This inclusion makes it problematic to prosecute those cases where PSIs were published without the revenge motive or without the intention to emotionally harm the victim. Such examples include PSI dissemination for pecuniary gain. While revenge pornography does cause a certain amount of emotional distress, including 'emotional distress' as an ingredient of the legal provision makes it near-impossible to prove the crime in a Court. On the other hand, states like Illinois, have focused the law on whether the perpetrator could have reasonably known or understood the lack of consent of the victim, during the dissemination. The former has proved problematic, especially in the USA.

Laws attempting to criminalise nonconsensual dissemination of intimate images are met with the challenges posed by the US Constitution's first amendment, guaranteeing the citizens a right to free speech. Any law that puts 'content-based restrictions on speech' is subjected to the strict scrutiny test. Government is rarely able to supersede the strict scrutiny test. Penal provision against revenge pornography laws must be created in a way, which is able to survive the test of strict scrutiny.

Much of the revenge pornography debate boils down to free speech versus right to be forgotten. The inclusion of disseminated PSIs as an expression of free speech can have problematic impacts in the context of a citizen's right to be forgotten. The US law is usually not accommodating of the right to be forgotten. In *Martin v. Hearst Corporation*, a U.S. court of appeals denied to have online articles about the arrest of three individuals removed, after such individuals were "*deemed to have never been arrested*" under state law of Connecticut. This

case, as well as the refusal by US Supreme Court to review this decision, indicates that US law will favour the right to free speech over the right to be forgotten.

Some have called for new and specific laws in USA to target the circumstances of nonconsensual dissemination of PSIs. Stokes, for example, argues that a special exception should be created u/s 230 of US-CDA itself, in order to open up the intermediaries to tortious claims. However, there are some authors who have specifically argued against it. Accordingly, to some, most proposals of reform are troubled with “internet exceptionalism”, where the internet is treated as a unique medium of perpetrating an offence.

Invasion of Privacy in Australia:

In Australian legal context, defamation law has proved ineffective against revenge pornography as truth is not a sufficient defence in all states. Action under Copyright laws can only be brought by a victim who happens to be the author of the video. Moreover, both criminal cases and civil cases are costly remedies. Australian penal laws were found insufficient in dealing with revenge pornography. As a result, the Commonwealth Senate Legal and Constitutional Affairs References Committee (‘Senate LACARC’) recommended that a new law be drafted to target non-consensual sharing of private or sexual images. The Australian Law Reform Commission (ALRC) suggested in direct contradiction to the Manila Principles, that intermediaries should be made liable under tort law and that a tortious liability be created for invasion of privacy.

A Humanitarian view of Europe:

In UK, most remedies in tort law and criminal law have failed to prevent takedown of the PSIs. Section 33(8) of the Criminal Justice and Courts Act (CJCA) 2015 provide for a *mens rea* element, which makes it incredibly difficult to prosecute individuals. Schedule 5 of the Act also excludes liability of intermediaries. Similarly, tort law or rather torts law, as is more prevalent in UK, as it is not possible to make each individual sharers of PSI liable legally.

Revenge pornography is also a human rights issue. UK Courts have held through multiple precedents that Article 8 of the European Convention on Human Rights shall have to be considered even in civil disputes between individuals. Section 6 of the Human Rights Act also obligates any ‘public authority’ including a Court or a tribunal to ensure adherence to the

ECHR. However, the protection of the victim of revenge pornography is also a part and parcel of this obligation.

Crown Prosecution Service Guidelines of 2015 provide for introduction of liabilities of the intermediaries in revenge pornography cases. In fact, making an intermediary liable is proposed to be one of the key measures in making them adopt technologies to stop uncontrolled dissemination of PSIs. Yet not all intermediaries have the necessary technology to be able to stop such dissemination or to be able to provide strong take down services.

Articles 12-14 of the E-Commerce Directive 2000/31/EC of the European Parliament makes those intermediaries and hosts liable for revenge pornography, who have knowledge of materials being posted. This knowledge may be proved to be existent for only those intermediaries who have specific websites designed for revenge pornography. However, most of the intermediaries would take the loophole of lack of proof of knowledge. If the victims of revenge pornography hold the copyright to their respective PSIs, they can request takedown of the same, stop the publication and broadcasting of the same and even control their distribution.

Unfortunately, the situation is vastly more complicated. Firstly, if the image has been modified, edited or even deep-faked, the depicted person will not be the copyright-holder. In fact, the perpetrator would be the copyright holder. Similarly, when the victim has been taped or photographed without her consent, she would not be the copyright holder. Only on those particular instances where the victim captures herself and later such image is disseminated without any creative modification, would she be the copyright holder. One of the first attempt at takedown came from Facebook, where a suggested Photo DNA technology would convert the original picture into a unique cryptographic hash function, thereby making it easy to report and prevent revenge pornography. However, this method would not be able to stop dissemination of such images on other sites across the internet.

The debate of right to be forgotten versus right to free speech in the context has fared better in the European context. The European Court of Justice (ECJ) in the case of *Google Spain v. AEPD and Gonzdlez*, decided that citizens had the right to be forgotten by requesting google to take down certain results. The Commission *Nationale de l'Informatique et des Libertes* (CNIL) decided deleting results from European nations were not sufficient and the website must take the search down from the domain page 'google.com' altogether.

India and combat of revenge pornography:

In India, female victimisation is not a new phenomenon. Such dissemination has targeted women more often than not. *‘Most of the crimes against women in India directly traceable to their inferior and subservient status, as sanctified by social values and ideas based on religion.’* Non-consensual dissemination is not an exception to this. Existing laws that can hope to combat revenge pornography are Section 67, 67A, 67B of the Information Technology Act of 2000 and the erstwhile Section 354C of the Indian Penal Code. Indian laws on cyber-crimes in general are evolving.

In *Manoj Dattatray Supekar v. State of Maharashtra* the aggrieved woman alleged that the man she was involved with, recorded videos of their intimate moments and sent the same to her relatives. However, the perpetrator was granted bail, citing the ground that the offence u/s 67A of the IT Act was punishable by only up to 5 years. In, *State (NCT of Delhi) v. Mahesh*, the Delhi High Court upheld a trial Court acquittal. The facts of the case were that the perpetrator forced the victim to disrobe herself under threat of physical harm and recorded her. He later disseminated the recording online. However, the trial Court judge held that there was no proof that it was the perpetrator who disseminated the video. As such, he was acquitted u/s 67A of IT Act.

In *Jaykumar Bhagwanrao Gore v. State of Maharashtra*, an MLA who was accused u/s 67 and 67A of the ITA, tried taking a plea that alleged SIM cards did not belong to his name. However, such plea was not considered and his anticipatory bail application was rejected.

In *X v. Union of India*, the victim’s images were shared in the website ‘www.xhamster.com’ by an unknown entity. It was claimed that the photographs were “*offensive by association*”. The Hon’ble Court appointed an expert in cyber law as amicus curiae so as to not “*permit itself to resign to the cat-and-mouse game of errant parties evading court orders by re-posting offending content across the world-wide-web, in an act of defiance and contumacy*”. Ultimately, the Court directed the search engines Google Search, Yahoo Search, Microsoft Bing and DuckDuckGo, to “globally de-index and de-reference from their search results the offending content as identified by its Web URL and Image URL, including de-indexing and de-referencing all concerned web-pages, sub-pages or sub-directories on which the offending content is found” as well as to proactively identify and disable access to any such similar or identical content on a global scale, on any other websites or any other online platforms. Hon’ble

Court clarified that non-adherence to these directions would render the intermediaries devoid of the protection u/s 79 of ITA and render them responsible u/s 85 of ITA.

Justice B.N. Srikrishna Committee recommended that the “right to be forgotten” should be added within the ambit of the “right to privacy” Ministry of Law and Justice included the ability of an individual to delink, or delete the disclosure of misleading, embarrassing or irrelevant personal information, in The Digital Personal Data Protection Bill, 2023.

In *X v. Union of India* 2021 SCC , the Hon’ble Court held that the intermediaries cannot reasonably be tasked with automatically pointing out offensive images and deleting it. This would cause an affront on the idea of free speech itself. The Apex Court as well, pointed out that “an intermediary cannot be allowed to apply its own mind to adjudge the legitimacy of online content”. Instead, the intermediaries have a duty to remove offensive content which has been decided as offensive after adjudication and which has been reported to them. The law with respect to intermediary responsibility vis-à-vis nonconsensual dissemination also includes the Information Technology rules, which casts a duty on the intermediary to take-down offensive content when the same has been reported as such. What would constitute such an offensive “imagery” is now open to judicial interpretation. Penal sections of 67, 67A and 67B also deal with punishing the perpetrator. Though convictions are extremely rare, the trial Court recently convicted a perpetrator who shared intimate images of a victim without her consent on a website allocated for pornographic content.

Conclusion:

The laws targeting the aforementioned dissemination has been enacted in India. However, the issue of proof, take-down method and prevention is still under judicial interpretation. There is a scope of a larger study to evaluate the best practices of foreign jurisdictions and see how far they fit the Indian legal patterns. Non-consensual dissemination of pictures or videos online is a typical form of cyber harassment, which attempts to victimize a person by dissemination of private pictures or videos. On the global scale, the terminology to describe this form of harassment itself is still evolving.

Before the enactment of the Bharatiya Nyaya Sanhita, 2023 (hereinafter BNS, 2023) non-consensual dissemination of sexual images was dealt with a combination of existing offences under the Indian Penal Code (hereinafter IPC) and the Information Technology Act (hereinafter

IT Act). Section 67A of the IT Act was used to tackle non-consensual dissemination of sexual images online. If the victim of such dissemination was a child, Section 67B would be attracted.

In cases of picture or video taken unbeknownst to the victim, and later disseminated online, the same would be dealt under section 354C read with section 67A of the IT Act. If the pictures were not disseminated or partially disseminated and an accompanying threat was used to extort the victim, then Sections 506 (criminal intimidation) would ordinarily also be used. The BNS has enacted the offence of voyeurism, exactly as it was defined earlier in the IPC, in Section 77.

A sharp increase in reported cybercrimes in India across all categories, indicate that this unique species of cyber harassment is likely to become a problem of increasing magnitude. NCRB data shows that in 2022 alone, 6896 cases have been registered for publication/ transmission of obscene or, sexually explicit act in electronic form. 1931 cases were registered u/s 67A, IT Act and 1166 cases were registered u/s 67B, IT Act, which deals with such transmission when the victims are children. Out of the cases registered under Section 67A and 67B, ITA, the chargesheet was submitted in only 1214 cases. It is sufficiently clear from NCRB data itself that accused persons seldom get convicted u/s 67A, 67B and allied sections. A total of 5430 cases were pending before the Courts in 2022 u/s 67A and 67B of IT Act. The number of cases abated by Court was only 4, in all of India. Clearly the mechanism leaves some things to be desired.

The non-consensual dissemination of sexual images through the internet is a significant challenge to the Indian legal system. As the use of digital technologies increase, so does its abuse. The efficacy of Indian legal framework in tackling non-consensual dissemination of sexual imagery through India is under scrutiny, especially since the rate of conviction is abysmal. Therefore, there is a need for a comprehensive legal policy and statutory provisions under the India's legal framework.

Notes:

1. Section 67 of the Information Technology Act(India) penalises publishing or transmitting obscene material in electronic form. It reads: *‘Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.’*

2. Section 67A of the Information Technology Act(India) penalises publishing or transmitting of material containing sexually explicit act, etc., in electronic form. It reads: *‘Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.’*

3. Section 67B of the Information Technology Act(India) penalises publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form. It reads: *‘Whoever,*

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and

on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form—

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes.

Explanation—For the purposes of this section, —children means a person who has not completed the age of 18 years.’

4. Section 354C of the Indian Penal Code punishes Voyeurism. It reads: ‘Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.’ However, recently the Bharatiya Nyay Sanhita (BNS) has replaced the Indian Penal Code.

References:

1. Sarah Esther Lageson, Suzy McElrath and Krissinda Ellen Palmer, Gendered Public Support for Criminalizing ‘Revenge Porn’ (2018) 14 Feminist Criminology 560
2. Sarah Cefai, ‘Humiliation’s Media Cultures: On the Power of the Social to Oblige Us’ (2020) 22 New Media & Society 1287
3. Samantha Bates, “Revenge Porn and Mental Health” (2016) 12 Feminist Criminology 22
4. Dr. N. V. Paranjape, *Studies in Jurisprudence and Legal Theory* (Eighth edition, Central Law Agency, 2016) 621-622
5. Jenna K. Stokes, ‘The Indecent Internet: Resisting Unwarranted Internet Exceptionalism Combating Revenge Porn’ (2014) 29 Berkeley Tech LJ 929; Lex Dymock & Charlotte van der Westhuizen, ‘A Dish Served Cold: Targeting Revenge in Revenge Pornography’ (2019) 39 Legal Stud 361
6. Nicolas Suzor, Bryony Seignior & Jennifer Singleton, ‘Non-Consensual Porn and the Responsibilities of Online Intermediaries’ (2017) 40 Melbourne Law Review 1057, 1059
7. Gautam Bhatia, *The Transformative Constitution* (Harper Collins Publishers, 2019) 218-219
8. V. N. Shukla, *Constitution of India* (Thirteenth edition, 2017) 215
9. *Maneka Gandhi v. Union of India* [1978] 1 SCC 248, AIR 1978 SC 597, 620
10. *Kharak Singh v. the State of UP and others* [1963] AIR 1295
11. *Justice K.S. Puttaswamy v. Union of India* [2018] AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1
12. Lex Dymock & Charlotte van der Westhuizen, ‘A Dish Served Cold: Targeting Revenge in Revenge Pornography’ (2019) 39 Legal Stud 361, 362

13. Using IP Rights to Protect Human Rights: Copyright for ‘Revenge Porn Removal’ (2020) 40 Legal Stud 442
14. Guy Aitchison and Saladin Meckled-Garcia, ‘Against Online Public Shaming: Ethical Problems with Mass Social Media’ (2021) 47 Social Theory and Practice 1, 2-3
15. Ava Schein, ‘When Sharing Is Not Caring: Creating an Effective Criminal Framework Free from Specific Intent Provision to Better Achieve Justice for Victims of Revenge Pornography’ (2019) 40 Cardozo Law Review 1953, 1955
16. Bates S, “Revenge Porn and Mental Health” (2016) 12 Feminist Criminology 22
17. Danielle Keats Citron & Mary Anne Franks, ‘Criminalizing Revenge Porn’ (2014) 49 Wake Forest L. Rev. 345, 346
18. Nicolas Suzor, Bryony Seignior & Jennifer Singleton, ‘Non-Consensual Porn and the Responsibilities of Online Intermediaries’ (2017) 40 Melbourne Law Review 1057, 1067
19. Mika Westerlund, ‘The Emergence of Deepfake Technology: A Review’ (2019) 11 Technology Management Review 39, 39-40
20. Ahmed Siddique, *Criminology Penology and Victimology* (seventh edition, EBC 2018) 531
21. State of West Bengal v. Animesh Boxi @ Ani Boxi @ Ani Bokshi (2018), <<https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2018/06/State-of-West-Bengal-v.-Animesh-Boxi.pdf>> accessed 25 April 2024
22. Leah S. Murphy, ‘When Free Speech and Privacy Collide: Why Strict Scrutiny Is a Poor Fit for Nonconsensual Pornography Laws’ (2021) 42 Cardozo Law Review 2577, 2579-2580
23. Mary Anne Franks, ‘Why We Need a Federal Criminal Law Response to Revenge Porn’, (*Concurring Opinions*, 15 February 2013), <<https://concurringopinions.com/archives/2013/02/why-we-need-a-federal-criminal-law-response-to-revenge-porn.html>> accessed 10 April 2024

24. 'Additional Developments' (2011) 26 Berkeley Tech LJ 765
25. Irina D. Manta, 'Gawking Legally' (2018) 41 Harv J L & Public Policy 117, 120
26. Ashley Johnson and Daniel Castro, 'Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved' (*Information Technology and Innovation Foundation*, 22 February 2021) <
<https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved/>> accessed 11 April 2024
27. Danielle Keats Citron & Mary Anne Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest L. Rev. 345
28. *Martin v. Hearst Corp.*, 777 F.3d 546, 551 (2d Cir. 2015)
29. Katherine Stewart, 'Looking Backward, Moving Forward: What Must Be Remembered When Resolving the Right to Be Forgotten' (2017) 42 Brook J Int'l L 843, 846
30. Nicolas Suzor, Bryony Seignior & Jennifer Singleton, 'Non-Consensual Porn and the Responsibilities of Online Intermediaries' (2017) 40 Melbourne Law Review 1057, 1061
31. Jenna K. Stokes, 'The Indecent Internet: Resisting Unwarranted Internet Exceptionalism Combating Revenge Porn' (2014) 29 Berkeley Tech LJ 929, 951
32. Debanjan Banerjee & T. S. Sathyanarayana Rao, '#Intimacy at Times of COVID-19: The Renewed Impetus Behind Cybersex' (2021) 3(1) Journal of Psychosexual Health 13, 15
33. Bates S, "Revenge Porn and Mental Health" (2016) 12 Feminist Criminology 22.
34. *X v. Union of India* (2021) SCC Online Del 1788, 91
35. *Shreya Singhal v Union of India* (2015) AIR 2015 SC 1523
36. The Digital Personal Data Protection Bill 2023

37. *Manoj Dattatray Supekar v. State of Maharashtra* (2016) SCC Online Bom 15449
38. *State (NCT of Delhi) v. Mahesh*, (2017) SCC Online Del 7956
39. *Jaykumar Bhagwanrao Gore v. State of Maharashtra*, (2017) SCC Online Bom 7283
40. *X v. Union of India*, (2021) SCC Online Del 1788