INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DEEPFAKE PORNOGRAPHY AND GENDER-BASED ONLINE VIOLENCE: A CRIMINAL LAW PERSPECTIVE

AUTHOR - KAROLIN C, LL.M (CYBERSPACE LAW AND JUSTICE), SCHOOL OF EXCELLENCE IN LAW, CHENNAI

BEST CITATION – KAROLIN C, EMPLOYMENT INEQUALITY IN THE AGE OF ARTIFICIAL INTELLIGENCE: CHALLENGES AND POLICY RESPONSES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (8) OF 2026, PG. 896-904, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I898

ABSRACT:

Deepfake pornography is a serious form of online violence against women. It uses intelligence to create fake but realistic sexual videos or images of women and girls without their permission. These fake videos are often shared online to hurt, blackmail or shame the victims causing pain, loss of reputation and health problems. From a law point of view this issue is studied to see how well current laws can deal with it. Most laws on harassment, privacy or revenge porn were made before deepfakes existed. As a result, they often fail to cover videos properly. It's hard to prove who made the video prove their intention and collect evidence in court. Many victims also face problems because the content spreads quickly across countries.

This paper looks at laws introduced in countries like the United States, United Kingdom, India and the European Union. It examines what works what's missing and the challenges in catching offenders and holding websites responsible. The study argues that clear specific laws are needed to treat -consensual deepfake pornography as a serious sexual offence. Stronger rules for media platforms quick removal of fake content better police powers and cooperation, between countries are also essential. The main goal should be to protect victims and stop this growing abuse while balancing free speech and privacy rights.

INTRODUCTION:

Deepfake pornography is a serious new problem created by artificial intelligence. It uses intelligence to create fake videos or photos that look real. These videos or photos show a person doing acts without their permission. Most deepfakes, 98% are pornographic. Most of them target women and girls. This is a form of violence against women. It hurts a person's privacy, dignity and safety. Victims feel stressed, depressed and ashamed. Their reputation also gets damaged. A single photo from media can be used to create these fake videos. Unlike revenge porn no real intimate photo is needed. Anyone can create it easily. Old laws are not enough to deal with this problem. They were made before AI existed. So it's hard to prove the crime find the person and take action. This issue needs to be looked at from a law point of view. We need to see the problems it creates the laws and what changes are needed to protect victims.

Deepfake pornography predominantly targets women and has become a new form of gender-based online violence, causing severe psychological, emotional, reputational, and social harm to victims. Therefore, this study critically analyses deepfake pornography as a form of gender-based online violence and examines the adequacy of existing criminal law mechanisms in addressing this growing digital threat.

RESEARCH OBJECTIVE:

- To understand the concept, technology, and scale of deepfake pornography and its

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

evolution as a new form of image-based sexual abuse.

 To analyse the nature and extent of harm caused by deepfake pornography to victims, particularly women and girls, from both legal and ethical perspectives.

 To undertake a comparative study of legal responses to deepfake pornography in selected jurisdictions (USA, UK, EU, and others) to identify best practices.

 To explore the ethical issues surrounding consent, dignity, privacy, objectification of women, and the responsibility of technology companies.

 To identify the major gaps and challenges in investigation, prosecution, and enforcement of laws relating to deepfake pornography.

CONCEPT OF DEEPFAKE TECHNOLOGY:

Deepfake technology is about using intelligence and deep learning to make fake audio, video and image content that looks real. The term deepfake comes from the words learning and fake which shows how neural networks are used to make fake digital media. This technology works with machine learning models like Generative Adversarial Networks, where one algorithm makes content and another checks if it is real which makes the output very convincing. By looking at expressions, speech patterns and body movements from a lot of data deepfake systems can copy real people very accurately.[1177]

At first deepfake technology was made for things like entertainment, education making movies and helping people with disabilities. In the movie industry it has been used to bring back actors make special effects better and help with translating movies into languages. As deepfake technology is used more and more it is also causing big legal and ethical problems. Some people are using deepfake technology to make speeches spread false information steal identities commit financial fraud and make pornographic content without consent. This is a problem in the digital world. Deepfake pornography is especially bad for women as it takes away their right to privacy, respect and control over their bodies.[1178]

Deepfakes are also hurting peoples trust in media and in the government. Fake videos and audio recordings can change the result of elections hurt people's reputations and spread stories. It is hard for police and courts to figure out what is real and what is made by intelligence, which makes it hard to use digital evidence in court. In India there are no laws about deepfakes but some laws like the Information Technology Act and the constitution do give some protection against deepfakes. So we need to make laws that stop the bad effects of deepfake technology while still allowing people to be creative and express themselves. We need to talk about deepfake technology and how it is used, like deepfake technology to make sure we are safe. The use of deepfake technology is an issue and we need to think about how to deal with it and that is why we need to know more, about deepfake technology.

DEEPFAKE PORNOGRAPHY AS GENDER-BASED ONLINE VIOLENCE:

Deepfake pornography is a problem on the internet. It is a type of violence against women that is made possible by technologies, like artificial intelligence and digital manipulation. People use computer programs to put someones face on dirty pictures or videos. This makes the fake pictures and videos look very real. Deepfake content is made using these computer programs that can put an individual's face onto images or videos making it look like the real thing. Deepfake pornography is getting worse because of these technologies. While deepfake technology may have legitimate applications in entertainment, education, and media production, its misuse in generating non-consensual pornographic content has created

[1177] Ian Goodfellow et al., "Generative Adversarial Nets," Advances in Neural Information Processing Systems 27 (2014): 2672–2680.

[1178] Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review 107, no. 6 (2019): 1753–1820.

serious legal, ethical, and human rights concerns. Studies indicate that the overwhelming majority of deepfake pornographic material targets women, often without their knowledge or consent, thereby reinforcing gender inequality and online abuse.[1179]

The problem of deepfake pornography is that it is an invasion of the person's private life it hurts their self-respect what people think of them and it is a big problem for their body and what they want to do with it. People who are victims of deepfake pornography often feel very bad they get very anxious they feel humiliated people do not want to be their friends anymore because of what's being said about them and they get hurt by what people think of them. Deepfake pornography is different from kinds of online bullying because it looks like it is real so people who see it do not know what is true and what is not. This makes the people who are victims feel even worse they get more upset. It is more likely that they will be bullied online blackmailed and lied about. Deepfake pornography is a problem because it is so realistic and that makes things worse, for the victims of deepfake pornography. In many cases, victims face long-term personal and professional consequences even after proving that the content is fake, as digital material can spread rapidly across social media and online platforms.[1180]

From a legal and feminist perspective, deepfake pornography represents a technologically advanced extension of sexual exploitation and violence against women in cyberspace. It reflects broader structural inequalities in digital spaces where women are disproportionately subjected to objectification, cyberstalking, and non-consensual sexual representation. Feminist scholars argue that such practices reinforce patriarchal control by reducing women's identities and bodies into objects for public consumption without consent. Therefore, deepfake pornography should not merely be viewed as a technological misuse but as a form of digital sexual violence that undermines substantive gender equality.[1181]

In India, although there is no dedicated legislation specifically criminalising deepfake pornography, certain provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and laws relating to obscenity, defamation, identity theft, and sexual harassment may provide partial remedies. Furthermore, constitutional protections under Article 21 guarantee the rights to privacy and dignity, as recognised in Justice K.S. Puttaswamy v. Union of India. However, the growing misuse of AI-generated explicit content highlights the urgent need for comprehensive legal reforms, stricter intermediary accountability, victim protection mechanisms, and technological safeguards to combat gender-based online violence effectively.[1182]

CRIMINAL LAW PERSPECTIVE ON DEEPFAKE PORNOGRAPHY:

Deepfake pornography is a problem for the law. This is because technology is getting better at making videos and pictures. Deepfakes are media made using artificial intelligence. A persons face, voice or body is changed to make it look real. It's not. In the case of pornography this technology is often used to make images or videos without someone's permission. Women and famous people are often targeted. This misuse of technology is a form of exploitation, harassment and humiliation. It can be considered a crime under laws about obscenity, cybercrime, defamation, identity theft and sexual harassment.[1183]

From a Criminal law perspective deepfake pornography is a form of sexual violence. It is a violation of a person's autonomy, privacy and

[1179] Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review 107, no. 6 (2019): 1753–1820.
[1180] Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age (New York: W.W. Norton & Company, 2022).
[1181] Catharine A. MacKinnon, "Pornography as Trafficking," Michigan Journal of International Law 26, no. 4 (2005): 993–1012.
[1182] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[1183] Matthew Groh et al., "Detecting Deepfake Videos: An Analysis of Human and Automated Approaches," Proceedings of the ACM on Human-Computer Interaction 6, no. CSCW2 (2022): 1–27.

dignity. The fake content looks very real which makes it seem authentic to viewers. Victims often suffer from anxiety, depression, emotional trauma and reputational harm. In cases deepfake pornography is used for blackmail, revenge or coercion especially against women. The fact that online content can be shared quickly and widely makes the damage, to victims even worse. Deepfake pornography causes psychological consequences. The permanent nature of content further intensifies the damage caused to victims.[1184]

Traditional criminal laws have a time dealing with deepfake pornography. The laws we have now were made to handle crimes, like obscenity, defamation and identity fraud not fake videos and pictures made by artificial intelligence. This makes it tough to prove someone did something on purpose find out who did it when they are hiding and figure out which countrys laws should apply when something bad happens on the internet. Furthermore, online intermediaries and social media platforms often lack effective mechanisms for the rapid detection and removal of manipulated sexual content, thereby allowing harmful material to circulate widely before legal intervention occurs.[1185]

In India, although no specific legislation directly criminalises deepfake pornography, several statutory provisions may provide partial legal remedies. Under the Information Technology Act, 2000, Sections 66E, 67, and 67A penalise violations of privacy and the electronic publication or transmission of obscene and sexually explicit material. Similarly, provisions under the Bharatiya Nyaya Sanhita, 2023 relating to defamation, outraging the modesty of women, stalking, and criminal intimidation may also apply. However, these laws do not adequately address the unique nature of AI-generated sexual abuse, especially regarding consent, synthetic identity manipulation, and platform accountability.[1186]

The constitutional dimension of deepfake pornography is equally important. The Supreme Court of India in Justice K.S. Puttaswamy v. Union of India recognised privacy as a fundamental right under Article 21 of the Constitution, including informational privacy and protection of personal dignity. Deepfake pornography directly infringes these rights by exploiting a person's image and identity without consent for sexually explicit representation. Therefore, criminal law must evolve to address emerging technological harms and ensure effective protection of victims in digital spaces.[1187]

INTERNATIONAL CRIMINAL LAW APPROACHES TO DEEPFAKE PORNOGRAPHY:

The quick spread of deepfake pornography has made things very tough for criminal law and global cyber governance. Deepfake pornography is when people use intelligence technologies to make or alter sexually explicit images, videos or audio recordings that show individuals in a false way without their permission. Since digital platforms let people share this kind of material across borders deepfake pornography has become a big cybercrime that cannot be stopped just by using laws from one country. So many countries and international institutions have started working on regulatory ways to stop the bad use of AI-generated sexual content while also protecting human rights, privacy and digital security.[1188]

Deepfake pornography is a problem for international criminal law because it goes against principles that are meant to prevent cybercrime protect human dignity, privacy rights and stop gender-based violence. Important human rights documents like the Universal Declaration of Human Rights and the Convention on the Elimination of All Forms of Discrimination Against Women say that people have the right to

[1184] Clare McGlynn and Erika Rackley, "Image-Based Sexual Abuse," Oxford Journal of Legal Studies 37, no. 3 (2017): 534–561.
[1185] Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI," Computer Law & Security Review 41 (2021): 105567.
[1186] Information Technology Act, 2000, Section 66E, 67, 67A.
[1187] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[1188] Henry Ajder et al., The State of Deepfakes: Landscape, Threats, and Impact (Amsterdam: Deeptrace Labs, 2019).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

dignity, equality, privacy and protection from exploitation. Deepfake pornography violates these rights by showing individuals, women, in a sexual way without their consent and by harassing them online. International organisations are starting to realise that technology-facilitated abuse is a form of gender-based violence that needs a legal response.[1189]

One important international instrument that can help stop deepfake pornography is the Budapest Convention on Cybercrime which helps countries work together to address cyber offences like identity theft, online exploitation and illegal digital content. Although the Convention does not specifically talk about deepfakes its rules about computer-related fraud, privacy violations and cyber-enabled crimes give a basis for countries to work together to investigate and prosecute these crimes. The Convention also encourages countries to help each other and work together internationally which is necessary because offenders often operate in many different countries.[1190]

Some countries have made laws to target deepfake pornography. In the United States states like Virginia, California and Texas have made laws that make it a crime to share non-consensual deepfake pornography and manipulated media. The United Kingdom also has laws that address this kind of conduct including laws about image-based abuse, harassment and malicious communications. The European Union has taken steps to regulate intelligence through the Artificial Intelligence Act, which tries to make companies that use high-risk AI systems be more transparent and accountable. These international developments show that more and more people recognise that AI-generated harms need legal regulation.[1191]

However international criminal law still has limitations when it comes to addressing deepfake pornography. Differences in laws from one country to another conflicts about which country has jurisdiction the fact that offenders can remain anonymous the lack of legal definitions and the difficulty of collecting digital evidence all make it hard to prosecute these crimes effectively. Moreover, many legal systems still rely on laws about obscenity and defamation that are not good enough to address the manipulation of synthetic media and AI-driven abuse. The fact that there are no global standards also creates gaps in enforcement which allows offenders to take advantage of countries with weaker cybercrime laws.[1192]

Therefore, international cooperation is essential for effectively combating deepfake pornography. States must work collectively to establish harmonised criminal laws, strengthen extradition mechanisms, regulate AI platforms, and promote technological tools for detecting manipulated content. International criminal law must evolve alongside emerging technologies to ensure the protection of privacy, dignity, and gender equality in the digital environment.

CHALLENGES IN INVESTIGATION AND PROSECUTION:

The way artificial intelligence and digital communication technologies are changing fast is making it really tough for people to investigate and prosecute cybercrimes especially when it comes to deepfake pornography and fake media. The police and the courts are facing a lot of procedural and legal problems when trying to deal with these kinds of crimes. The fact that artificial intelligence can create realistic fake content and that the internet is everywhere is showing that our old laws are not good enough to handle these new digital crimes.

One of the problems is figuring out what is real and what is not. Deepfake technologies use smart machine learning systems to make fake videos, pictures and audio recordings that look and sound real. This makes it very hard for

[1189] Universal Declaration of Human Rights, arts. 1, 12; Convention on the Elimination of All Forms of Discrimination Against Women, art. 5.
[1190] Budapest Convention on Cybercrime, Council of Europe Treaty No. 185
[1191] Artificial Intelligence Act, European Union, 2024.
[1192] Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for," Duke Law & Technology Review 16, no. 1 (2017): 18–84.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

investigators to tell what is fake. What is not. Because these technologies are changing fast the tools we use to investigate are becoming outdated quickly which makes it even harder to solve these crimes.

Another big problem is that the people who make and share deepfake pornography often hide their identities by using communication services, fake social media accounts and special networks that make it hard to track them down. This makes it very difficult to catch these people and get evidence that can be used in court. Sometimes the fake content is. Shared on platforms that operate in many different countries, which can cause problems and delays when trying to investigate.[1193]

It is also hard to use evidence in court because it has to be real not changed and believable. With deepfake technologies people are starting to doubt the accuracy of digital evidence. This has led to a problem where people who are accused of crimes can claim that the evidence against them is fake even if it is not. This makes it harder for prosecutors to prove that someone is guilty.

We also do not have enough laws to deal with these kinds of crimes. Many of our laws were made before artificial intelligence and deepfakes existed so they do not specifically address these crimes. In India for example we have laws that deal with things like obscenity and identity theft. We do not have a law that specifically deals with deepfake pornography. This can make it confusing and uncertain when trying to classify and prosecute these crimes.

Many people who are victims of these crimes are also afraid to report them because they are afraid of being embarrassed hurting their reputation for being harassed online. This means that many of these crimes are not reported, which makes it easier for the people who commit them to get with it. When harmful content is not removed from the internet quickly it can also cause lasting psychological harm to the victims.[1194]

To deal with these problems we need to have tools and training for our police and courts we need to work together internationally and we need to make new laws that address these crimes. We also need to make sure that the companies that operate platforms do more to detect and remove harmful content quickly. These are the things we need to do to make sure that we can investigate and prosecute crimes effectively and protect people's rights, in the age of artificial intelligence and digital manipulation.

HUMAN RIGHTS DIMENSIONS OF ONLINE GENDER VIOLENCE:

Online gender violence is a concern for human rights in today's digital world. This is because social media, artificial intelligence and online communication are used much. It includes things like cyberstalking, online sexual harassment and revenge porn. There is also deepfake porn hate speech, doxxing and sharing images without consent. These acts are mostly against women and gender minorities. Although these crimes happen online they affect victims personal, social and work lives. Online gender violence is not a cybercrime problem. It is also a violation of rights like dignity, privacy, equality and freedom, from discrimination. These rights are recognised around the world.

One of the most fundamental rights affected by online gender violence is the right to privacy and dignity. International human rights instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights guarantee protection against arbitrary interference with privacy, honour, and reputation.[1195]

Online abuse involving deepfake pornography or non-consensual sharing of content directly breaks these protections. It exposes victims to humiliation and damage to their reputation. In

[1193] Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes (Boston: Northeastern University Press, 2012).

[1194] Clare McGlynn and Erika Rackley, "Image-Based Sexual Abuse," Oxford Journal of Legal Studies 37, no. 3 (2017): 534–561.

[1195] Universal Declaration of Human Rights, art. 12; International Covenant on Civil and Political Rights, arts. 17, 19

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Justice K.S. Puttaswamy v. Union of India, the Supreme Court of India recognised privacy as a fundamental right under Article 21 of the Constitution and held that dignity, autonomy, and informational control are essential aspects of personal liberty. This landmark judgment significantly strengthened constitutional safeguards against digital exploitation and misuse of personal information.[1196]

Online gender violence also undermines the right to equality and non-discrimination. In Vishaka v. State of Rajasthan, the Supreme Court recognised sexual harassment as a violation of women's fundamental rights to equality, dignity, and life under Articles 14, 15, and 21 of the Constitution. Although the case focused on workplace harassment, the principles laid down are equally relevant to digital spaces where women face harassment and intimidation through online platforms.[1197]

Another important human rights concern relates to freedom of expression and safe participation in digital spaces. In Shreya Singhal v. Union of India, the Supreme Court struck down Section 66A of the Information Technology Act, 2000 on the ground that it violated freedom of speech and expression under Article 19(1)(a). At the same time, the Court acknowledged that lawful restrictions may be imposed to prevent abuse, incitement, and unlawful online conduct. This judgment demonstrates the challenge of balancing freedom of expression with protection from digital harassment and gender-based violence.[1198]

The court made another decision in the case of Bodhisattwa Gautam v. Subhra Chakraborty. The Supreme Court said that violence against women is wrong because it violates their human rights and dignity. This case was about violence in a different situation but the rules that were made are still useful when talking about online gender violence. This is because digital abuse also hurts peoples autonomy, dignity and mental well-being.[1199]

In the case of State of Punjab v. Gurmit Singh the Court said that victims of crimes need to be protected from feeling ashamed in public and from being victimized again. This is very important in cases where people share sexual videos or pictures without permission or create fake sexual content, which is called deepfake sexual content. This reasoning is highly relevant in cases involving revenge pornography and deepfake sexual content, where victims often face societal stigma and emotional trauma.[1200]

Therefore, addressing online gender violence requires a comprehensive human rights-based approach involving stronger cyber laws, victim-centred remedies, digital literacy, and platform accountability. Governments and international institutions must ensure that technological advancements do not become instruments of exploitation and discrimination. Effective legal regulation and judicial protection are essential to safeguard human dignity, privacy, equality, and freedom from violence in the digital age.

RECOMMENDATIONS:

The problem of intelligence being used to create fake porn videos is a very serious issue. This is a form of violence against women that happens online. The increasing misuse of artificial intelligence in creating deepfake pornography has emerged as a serious form of gender-based online violence, requiring urgent legal and policy intervention. Existing criminal laws and cyber regulations in many countries, including India, are inadequate to address the unique challenges posed by AI-generated sexual content.

One of the primary recommendations is the enactment of dedicated legislation specifically criminalising deepfake pornography and synthetic sexual content. Current legal provisions relating to obscenity, defamation, identity theft, and cyber harassment provide only indirect

[1196] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
[1197] Vishaka v. State of Rajasthan, (1997) 6 SCC 241.
[1198] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[1199] Bodhisattwa Gautam v. Subhra Chakraborty, (1996) 1 SCC 490
[1200] State of Punjab v. Gurmit Singh, (1996) 2 SCC 384

remedies and fail to adequately address issues such as consent, digital manipulation, and AI-generated exploitation. Special legislation should clearly define deepfake offences, prescribe stricter punishments, and recognise non-consensual AI-generated pornography as a form of digital sexual violence and gender-based abuse.

Another important recommendation is the strengthening of cybercrime investigation infrastructure. Governments should establish specialised cybercrime units equipped with advanced digital forensic technologies capable of detecting manipulated media and tracing offenders. Police officers, prosecutors, and judicial authorities should receive continuous training regarding artificial intelligence, digital evidence, and cyber forensic procedures.

International cooperation is equally important because deepfake crimes frequently involve cross-border digital platforms and anonymous offenders operating from different jurisdictions. Further, governments should promote ethical AI governance regulate the development and use of synthetic media technologies. AI developers and technology companies should follow principles of transparency, accountability, privacy protection, and human rights compliance. Public awareness programmes and digital literacy campaigns should also be conducted to educate individuals regarding consent, cyber safety, and the risks associated with manipulated media.

Finally, constitutional values relating to dignity, privacy, equality, and freedom from violence must guide legal responses to deepfake pornography. Therefore, effective criminal law reform, technological regulation, and human rights protection are essential to address deepfake pornography and ensure safer digital environments for all individuals.

CONCLUSION:

Deepfake pornography is a problem in the digital world and it is a very bad thing that happens to people online. When someone uses computers to make sexual videos or pictures without asking it hurts a person's privacy, dignity and reputation. This mostly happens to women. It can make them very upset, scared and embarrassed in front of others. This includes introducing specific statutory provisions criminalizing non-consensual deepfake content, strengthening cyber forensic capabilities, imposing stricter obligations on online platforms, and enhancing international cooperation in cyber investigations. The government should make it easier to investigate these crimes make sure the people who run websites are more responsible and teach everyone about how to be safe. A proper balance between technological development and protection of human rights is necessary to ensure a safer online environment for everyone.

REFERENCES:

1. Ian Goodfellow et al., "Generative Adversarial Nets," Advances in Neural Information Processing Systems 27 (2014): 2672–2680.
2. Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age (New York: W.W. Norton & Company, 2022).
3. Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review 107, no. 6 (2019): 1753–1820.
4. Matthew Groh et al., "Detecting Deepfake Videos: An Analysis of Human and Automated Approaches," Proceedings of the ACM on Human-Computer Interaction 6, no. CSCW2 (2022): 1–27.
5. Clare McGlynn and Erika Rackley, "Image-Based Sexual Abuse," Oxford Journal of Legal Studies 37, no. 3 (2017): 534–561.
6. Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI," Computer Law & Security Review 41 (2021): 105567.

7. Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes (Boston: Northeastern University Press, 2012).
8. Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for," Duke Law & Technology Review 16, no. 1 (2017): 18–84.
9. Henry Ajder et al., The State of Deepfakes: Landscape, Threats, and Impact (Amsterdam: Deeptrace Labs, 2019).
10. Bobby Chesney and Danielle Citron, "Disinformation on Steroids: The Threat of Deepfakes," Foreign Affairs 98, no. 1 (2019): 147–155.
11. Gautam Bhatia, Privacy in the Age of Technology (Oxford University Press, 2019).
12. Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books, 2nd edn., 2006).