LEGAL PERSPECTIVE ON DEEPFAKES: AN EMPIRICAL RESEARCH AMONG UNIVERSITY STUDENTS IN DEHRADUN

M Dornis Suveda Menon, ICFAI University Dehradun

ABSTRACT

This research paper investigates the legal implications of the recent phenomenon of "deepfakes," which are artificial intelligence-generated media that alter audiovisual content. It brings to light the growing prevalence of deepfakes across different sectors i.e., politics, entertainment, personal privacy. Discussing the serious ethical, social and legal implications of this technology by conducting an empirical survey among university students of Dehradun. This paper also evaluates if current legal frameworks are indeed sufficient to mitigate the threats faced by deepfakes in daily life by analysing existing court rulings and existing statutory legislations.

Keywords: Deepfakes, legal awareness, cybercrime, privacy

1. INTRODUCTION:

Deepfakes, a type of Artificial Intelligence (AI), are synthetic media created by neural networks that merge, replace, and modify photos or videos, resulting in content that appears legitimate but is completely fabricated. The term "deepfake" combines "deep learning" and "fake"[1] (Rana & Sung, 2020) Deepfakes are distinguished by their broad reach, pervasive scale, and advanced complexity, which enables virtually anyone with a computer to make convincingly realistic films that closely mimic authentic media[2]. (Fletcher, 2018). Although the technology was first used for entertainment, its growing sophistication has led to its application in more detrimental and malevolent domains, including fraud, harassment, and political manipulation. Deepfakes will probably be used more frequently in the future for market manipulation, political sabotage, terrorist propaganda, extortion, revenge porn, bullying, fake video evidence in court, and fake news[3]. (Maras & Alexandrou, 2019).

2. PURPOSE OF THE STUDY:

The purpose of this study is to ascertain whether college students are aware of deepfakes—AI-generated content that alters photos and videos—and the legal safeguards afforded to anyone impacted by such content. The purpose of the study is to explore a number of aspects of students' knowledge, including their awareness of legal provisions on deepfakes and other remedies such as how to report and seek redressal for the misuse of deepfake content, and their personal experiences with manipulated photos and videos. Key research questions focus on students' individual experiences with manipulated media, how frequently they come across such content and their awareness of platforms that facilitate the creation of deepfakes. The survey conducted also looks at how well-informed students are about the legal options accessible to them, including how to report issues, if they can get compensation, and pertinent laws in India, including the Information Technology Act of 2000. The study also investigates how students view the possible harm that deepfakes could do to people's reputations and

[1] M. S. Rana & A. H. Sung, Deepfakestack: A Deep Ensemble-Based Learning Technique for Deepfake Detection, in 2020 7TH IEEE INTERNATIONAL CONFERENCE ON CYBER SECURITY AND CLOUD COMPUTING (CSCLOUD)/2020 6TH IEEE INTERNATIONAL CONFERENCE ON EDGE COMPUTING AND SCALABLE CLOUD (EDGECOM) 70 (2020).

[2] Fletcher, J. 2018. Deepfakes, Artificial Intelligence, and Some Kind of Dystopia: The New Faces of Online Post-Fact Performance. Theatre Journal, 70(4): 455–471. Project MUSE, https://doi.org/10.1353/tj.2018.0097

[3] Maras, M. H., & Alexandrou, A. 2019. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. International Journal of Evidence & Proof, 23(3): 255–262. https://doi.org/10.1177/1365712718807226

general well-being, as well as how government restrictions might help curb the abuse of this technology. The purpose of the research is to evaluate students' knowledge gaps through these questions.

3. OVERVIEW:

The paper initially outlines the deepfake technology examines its quick development, potential uses, and implications for digital media privacy, reputation, and cybercrimes. The report then explores the legal framework, focusing on pertinent Indian statutes that address the harms caused by deepfakes, such as the Information Technology Act of 2000. Based on the results of the empirical data collected the study ends with suggestions for improving legal knowledge and digital literacy to better prepare people to identify and address the threats posed by deepfake technology.

4. BACKGROUND

4.1 Explaining deepfakes

The term ‘deepfake’ was originally coined by a Reddit user who used ‘Face-swapping’ technology to superimpose celebrities' faces on pornographic videos[4]. Deepfakes are classified into numerous categories, including face replacement, speech synthesis, and shallowfakes. While speech synthesis employs artificial intelligence to mimic voices, face replacement entails swapping out one person's visage for another. Conversely, shallowfakes use simple editing methods that don't depend on complex algorithms[5]. (Europol 2020) The game-changing factor of deepfakes is the scope, scale, and sophistication of the technology involved (Fletcher, 2018) which are developed through Generative Adversarial Networks[6].

There is growing concern about the applications of deepfake technology due to its rapid development. These issues are mostly related to the development of a distrustful atmosphere and the potential for dishonest hackers and con artists to take advantage of weak and gullible

[4] Hannah Smith and Katherine Mansted, Weaponised deep fakes : National security and democracy (Australian Strategic Policy Institute 2020)
[5] Europol (2020) In: Malicious uses and abuses of artificial intelligence. Available via Europol. https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf. Accessed 15 Feb 2022
[6] Todd C. Helmus, Artificial Intelligence, Deepfakes, and Disinformation : A Primer (RAND Corporation 2022)

people[7]. These technologies are becoming more widely available; anyone with minimal technical knowledge can now produce convincing fake material thanks to user-friendly programs like FakeApp, Zao, FaceSwap, and Face2Face[8]. (Alanazi, S., Asif, S 2024) One no longer has to be an expert in machine learning with a lot of time and computing resources in order to create a deepfake[9].(Fallis, D 2021)

With the rise of social media and the widespread sharing of photos and videos, deepfake developers have found it simple to collect images from a specific person's account in order to create a doctored porn video[10]. There was a substantial increase in the visibility of deepfakes, which increased tenfold globally in 2022–2023[11]. The World Economic Forum's Global Risks Report 2024 names misinformation and disinformation as the biggest threat facing the world during the next two years[12].

4.2 How deepfakes have been used

Deepfakes are primarily used in four contexts: political campaigns, pornography, business applications to lower transaction costs, and creative works such as memes and movies[13]. 2019 research on the rise in deepfake videos since their 2017 analysis was published by Sensity AI's Deeptrace Lab[14]. According to the analysis, the number of deepfakes has increased by about 100%, from 7,964 videos in December 2018 to 14,678 videos in September 2019 (Ajder et al. 1-27). This number increased to 52,000 by the middle of 2020. According to the 2019 research, 96% of deepfakes were sexual, and where the ratio is 100 percent female-

[7] Vig, Shinu. "Regulating Deepfakes: An Indian perspective." Journal of Strategic Security 17, no. 3 (2024) : 70-93. DOI: https://doi.org/10.5038/1944-0472.17.3.2245 Available at: https://digitalcommons.usf.edu/jss/vol17/iss3/5

[8] Alanazi, S., Asif, S. Exploring deepfake technology: creation, consequences and countermeasures. Hum.-Intell. Syst. Integr. (2024). https://doi.org/10.1007/s42454-024-00054-8

[9] Fallis, D. The Epistemic Threat of Deepfakes. *Philos. Technol.* **34**, 623–643 (2021). https://doi.org/10.1007/s13347-020-00419-2

[10] Dave Lee, Deepfakes Porn Has Serious Consequences, BBC News (Feb. 3, 2018), https://www.bbc.com/news/technology-42912529, accessed Apr. 15, 2020.

[11] Nupura Ughade, *Are Deepfakes Illegal? Overview Of Deepfake Laws And Regulations* (Hyperverge, Aug. 12, 2024)

[12] World Economic Forum, "Global Risk Report 2024," accessed May 14, 2024, https://www.weforum.org/publications/global-risks-report-2024/.

[13] Edvinas Meskys, Aidas Liaudanskas, Julija Kalpokiene, Paulius Jurcys, Regulating Deep Fakes: Legal and Ethical Considerations, 15 J. INTELL. PROP. L. & PRAC. 24 (2020).

[14] DeepTrace, The State of Deepfakes, Landscape, Threats, and Impact https://regmedia.co.uk/2019/10/08/deepfake_report.pdf ↑

based, (Ajder et al. 1-27)[15].

GANs were initially used to produce deepfake sex videos, especially celebrity and revenge porn deepfakes. Usually posted after a relationship ends, revenge porn consists of sexually explicit content intended to degrade, threaten, or hurt someone[16]. Face-swapped celebrity porn, which includes superimposing photographs of celebrities on the bodies of people engaging in sexual actions, is another type of deepfake sex material[17]. Recently, a number of Indian celebrities have been the targets of deepfakes, including Alia Bhatt, Katrina Kaif, Shraddha Kapoor, Kajol, and Rashmika Mandanna. Mandanna's face was cut into a viral video of a woman in a black dress in an elevator, which infuriated the public, while Alia Bhatt's face was superimposed onto another woman's body in another viral video[18].

BuzzFeed released a deepfake video of President Obama on April 17, 2018[19], demonstrating how easy sentences can be made up by mimicking his voice in strange ways. Deepfakes can interfere with democratic procedures like election campaigns[20] or depict fictitious occurrences like staged terrorist attacks. They have the potential to worsen social divisions, undermine faith in democratic institutions, and endanger national security or international relations if employed by adversarial regimes. A video message featuring Ukrainian President Volodymyr Zelensky pleading with Ukrainians to surrender and lay down their weapons appeared on social media in March 2022.

During the 2020 Delhi Legislative Assembly elections, two videos of Bharatiya Janata Party candidate Manoj Tiwari appeared online[21]. Tiwari was shown in the videos criticising the ruling Aam Aadmi Party administration. Deepfake technology was used to alter these videos.

The unauthorized use of personal information by deepfake information service

[15] Ajder, Henry, et al. Deeptrace. The State of Deepfakes: Landscape, Threats, and Impact, 2019, pp. 1–27, www.regmedia.co.uk/2019/10/08/deepfake_report.pdf.
[16] DK Citron, MA Franks, 'Criminalizing Revenge Porn' (2014) 49(2) Wake Forest Law Review 345.
[17] PHayward,ARahn, 'OpeningPandora'sBox:pleasure,consentandconsequenceintheproduction and circulation of celebrity sex videos' (2015) 2(1) Porn Studies 49.
[18] Shuchi Nagpal, *Deepfakes & Cyber Law* (Asian School of Cyber Laws, Feb. 6, 2024), https://www.asianlaws.org/blog-post.php?url=deepfakes-and-cyber-law.
[19] BuzzFeedVideo, 'You Won't Believe What Obama Says In This Video!' (17 April 2018) accessed on 31 August 2019; CSilverman, 'Barack Obama-Jordan Peele Video' BuzzFeed (17 April 2018) accessed 7 September 2019.
[20] R. Green, 'Counterfeit Campaign Speech` (2019) 70 Hastings Law Journal 1445, 1457
[21] D.H. Web Desk, "Deepfake Videos Were Used for the First Time in India by BJP: Report," Deccan Herald (Feb. 21, 2020)

providers and users worries people[22]. Deepfake impersonation can damage a person's or an organization's reputation. Deepfakes, which are false comments or acts attributed to someone, can have detrimental long-term effects. The financial industry poses a serious concern as well, as unsuspecting consumers are tricked or intimidated into sending money to the criminal's account with deepfakes[23].

4.3 Legal and Ethical Implications of Deepfakes

The *Delhi High Court in Titan Industries Ltd. v. Ramkumar Jewellers*[24] decided that if the plaintiff has a right in the persona of a human being and the celebrity can be recognized from the infringement by the infringer, then the celebrity's rights can be enforced in India. *Sonu Nigam v. Amrik Singh*[25] the Bombay High Court granted Sonu Nigam an injunction for making misleading assertions about him in promotional posters, even though it acknowledged his celebrity rights.

In the case of *Anil Kapoor v. Simply Life India and Ors*[26]. Bollywood actor Anil Kapoor launched a lawsuit in reaction to the production of deepfake content utilizing his voice and likeness by artificial intelligence. Emojis, ringtones, GIFs, and even sexually explicit stuff were all included in this content. The Delhi High Court offered crucial protection for an individual's identity and personal characteristics against abuse in the matter. Especially when it came to AI technologies used to create deepfakes. The Court issued an ex-parte order, prohibiting sixteen businesses from utilizing artificial intelligence (AI) capabilities to profit off the actor's name, likeness, and image. In the case *Amitabh Bachchan v. Rajat Negi and Ors*[27], Mr. Amitabh Bachchan was granted an ad interim in rem injunction by the Delhi High Court to prevent the unapproved use of his personal characteristics and personality rights, such as his voice, name, picture, and resemblance, for commercial advantage. This decision strengthened the safeguards against the exploitation of a person's personal qualities for profit.

[22] Weiyin Hong and James YL Thong, "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," MIS Quarterly (2013): 275-298.
[23] Vig, Shinu. "Regulating Deepfakes: An Indian perspective." Journal of Strategic Security 17, no. 3 (2024) : 70-93. DOI: https://doi.org/10.5038/1944-0472.17.3.2245
[24] 2012 SCC OnLine Del 2382
[25] Civil Suit No. 372 of 2013, High Court of Bombay
[26] 2023 LiveLaw (Del) 857
[27] 2022 SCC OnLine Del 4110

4.4 Government advisory relating to deepfakes

On November 7, 2023, the Union Government issued a key advisory[28] to major social media intermediaries, encouraging them to take firmer action against disinformation and deepfakes, in a significant move to combat the growing threat of these types of content. According to the advisory, these platforms must apply due diligence and reasonable attempts to find and eliminate deepfakes and false material that contravenes user agreements and the material Technology (IT) Rules, 2021. Platforms are required by law to take down any content that has been reported within 36 hours of receiving a report, whether from users or government officials. Minister of State for Electronics and Information Technology Shri Rajeev Chandrasekhar reaffirmed that online platforms are required by law to take prompt, decisive action. In order to guarantee access to remedies under the IT Rules, the Minister further urged those impacted by deepfakes to submit First Information Reports (FIRs) to their local police.

In concurrence to the advisory, Facebook launched a project to detect and combat deepfakes[29]. Google and Pornhub have taken action against deepfake by banning and removing involuntary synthetic pornographic movies and images that are produced using deepfake technology[30]. Other websites, like Reddit and Gfycat, have also taken proactive measures to eliminate any non-consensual deepfakes and have opposed the use of the technology to create sexual photographs[31].

4.5 Existing Legal Frameworks and Challenges

There is currently no legislation in India that particularly addresses the issue of deepfakes. But the existing legislative statutes can be used in case incidents occur relating to deepfakes.

- IPC Section 499 - Defamation --> IT Act Section 66D - Cheating by personation using computer resource

[28] Press Information Bureau, Ministry of Information and Broadcasting, Government of India, Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes [Press Release], PIB Delhi (Nov 7, 2023), https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1975445.
[29] Elizabeth Culliford, Facebook, Microsoft Launch Contest to Detect Deepfake Videos, Reuters (Sept. 6, 2019, 3:27 AM), https://www.reuters.com/article/us-facebook-microsoft-deepfakes/facebook-microsoft-launch-contest-to-detect-deepfake-videos-idUSKCN1V0Q2T5.
[30] Matthew Beard, To Fix the Problem of Deepfakes We Must Treat the Cause, Not the Symptoms, The Guardian (July 23, 2019, 3:30 AM), https://www.theguardian.com/commentisfree/2019/jul/23/to-fix-the-problem-of-deepfakes-we-must-treat-the-cause-not-the-symptoms.
[31] Ankita Aseri, Overhauling Publicity Rights vis-à-vis Deepfakes - Truth Disrupted, 5 JIPL (2020) 15.

- IPC Section 500 - Punishment for defamation --> IT Act Section 66D - Cheating by personation using computer resource

- IPC Section 469 - Forgery for purpose of cheating --> IT Act Section 66C - Identity theft

- IPC Section 420 - Cheating and dishonestly inducing delivery of property --> IT Act Section 66D - Cheating by personation using computer resource

- IPC Section 384 - Extortion --> IT Act Section 66D - Cheating by personation using computer resource IPC Section 503 - Criminal intimidation --> IT Act Section 67 - Publishing obscene material in electronic form

- IPC Section 506 - Criminal intimidation --> IT Act Section 67 - Publishing obscene material in electronic form

- IPC Section 292- Sale, etc.., of obscene books etc.

- IPC Section 292-A. Printing, etc., of grossly indecent or scurrilous matter or matter intended for black mail.

- Copyright Act, 1957** * Section 51: Penalty for infringement of copyright

More stringent actions can be against those who transmit such videos when related to child porn[32]. Such offences are punishable under Protection of Children from Sexual offences Act, 2012. IT Act also explicitly banns child pornography[33].

Information Technology Rules, 2011

Deepfakes can be addressed by a number of regulations in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which are governed by the Information Technology Act, 2000. Although deepfakes are not directly mentioned in the regulations, processing sensitive personal data, including pictures and biometric information (Rule 4), which are frequently utilized in the

[32] Carl Ohman, Introducing the Pervert's Dilemma: A Contribution to a Critique of Deepfake Pornography, 22 Ethics & Inf. Tech. 133 (2020).
[33] Information Technology Act 2000, S. 67-B

construction of deepfakes, requires express consent. The regulations also require timely data breach notifications (Rule 7) to alert people if their personal data is misused and reasonable security methods (Rule 3) to prevent unauthorized access to such data. These safeguards, together with the duty to delete or anonymize data when it is no longer required (Rule 6), form a legal framework to limit the improper use of personal data in deepfakes.

Digital Personal Data Protection Act of 2023 (DPDPA)

The Digital Personal Data Protection Act of 2023 (DPDPA) establishes a vital legal framework for tackling privacy issues, especially those posed by new technologies such as deepfakes. Although deepfakes are not specifically addressed in the Act, a number of its provisions potentially lessen their effects.

Section 5 demands explicit consent for the collection and utilization of personal data, including sensitive data, such as biometric information (facial photos or voice recordings), which is routinely exploited in deepfake development. Section 12 grants individuals the right to erasure, allowing them to request the removal of personal information used in illegitimate deepfakes. While Section 24 enforces Data Protection Impact Assessments for sensitive data processing, which may assist uncover and reduce the risks of deepfake-related damages, Section 17 mandates data breach notifications, guaranteeing that people are notified if their data is misused. Growing doubts have been raised over the Digital Personal Data Protection Act, 2023's adequacy in tackling the emergence of deepfake technology in India. The necessity for more robust legal safeguards to safeguard people's rights against the exploitation of their personal information in the production of deepfakes and this legislative vacuum have been acknowledged by the courts.

One such instance is the August 28, 2024, Delhi High Court order, which drew attention to the legal loophole and underlined the need for immediate judicial action to protect the basic rights protected by the Indian Constitution. The court's action highlights the urgent need for legislative revisions to meet the particular risks posed by deepfakes and guarantee that people's privacy and dignity are sufficiently safeguarded in the digital era.

5. RESEARCH METHODOLOGY

This study involves a review of the literature available on deepfakes as well as the legal

provisions under which crimes using deepfakes can be covered, we also conducted an empirical approach is used, with a survey method administered via Google Forms, to examine university students' awareness of deepfakes, understanding of the risks involved, and knowledge of the legal tools available to resolve these issues. Both quantitative and qualitative data were gathered using the survey approach, which shed light on students' knowledge of deepfake technology, their opinions of its possible negative effects, and their knowledge of victims' legal options. Based on the survey's empirical results, the study ends with suggestions for improving legal knowledge and digital literacy to better prepare people to identify and address the threats posed by deepfake technology.

6. PRESENT STUDY

This study is limited to the University students of Dehradun.

6.1 Research Objectives

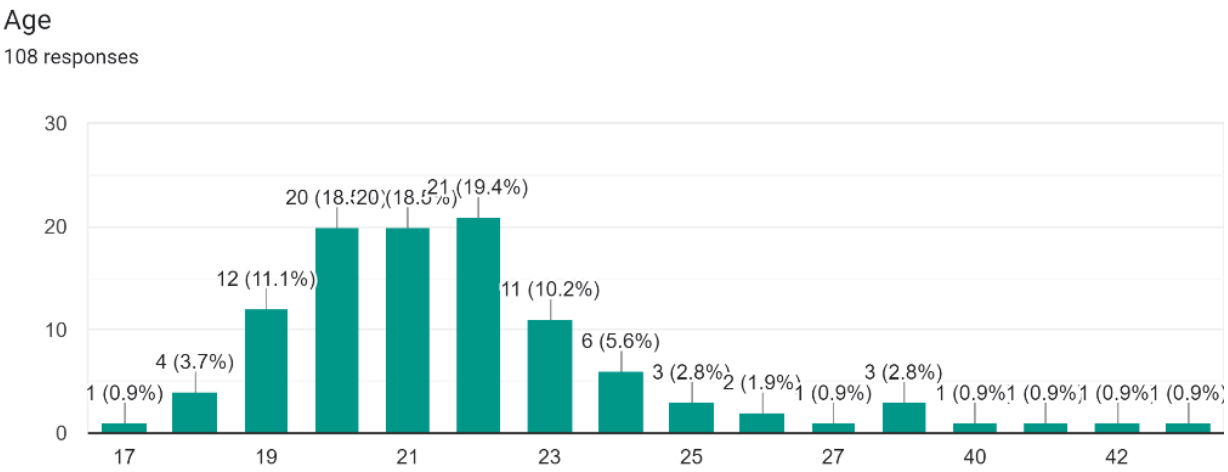
The objectives of this present study are as follows:

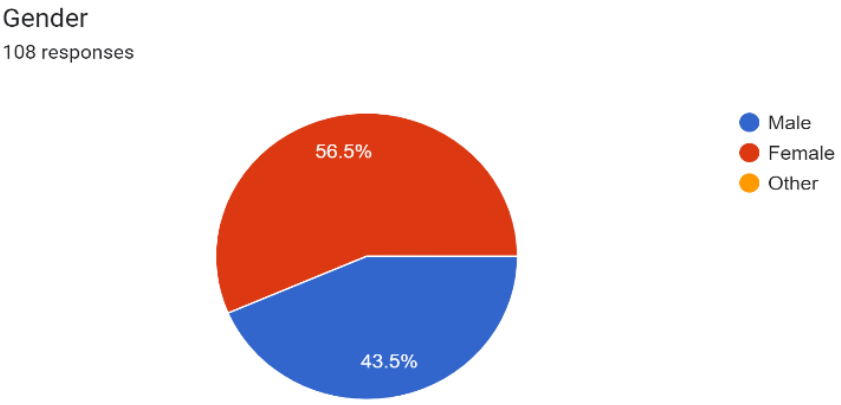
1. To assess legal awareness of students on provisions relating to deepfakes.
2. To explore the frequency of deepfake usage in daily life
3. To evaluate the groups vulnerable to deepfake and hear first-hand experiences of those affected.
4. To spread awareness as to how such cybercrimes can be addressed.

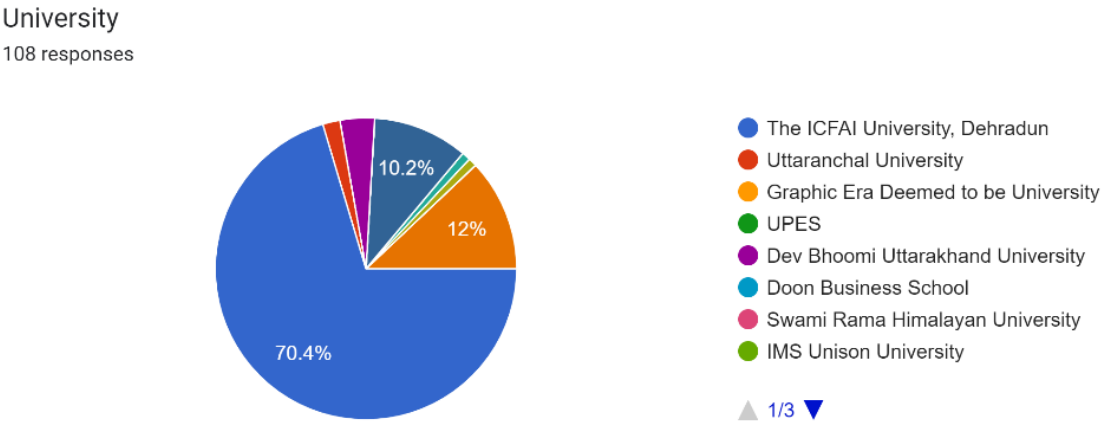
6.2 Hypothesis

University students lack sufficient knowledge about the legal measures and protections available to them when encountering deepfakes.

7. DATA ANALYSIS

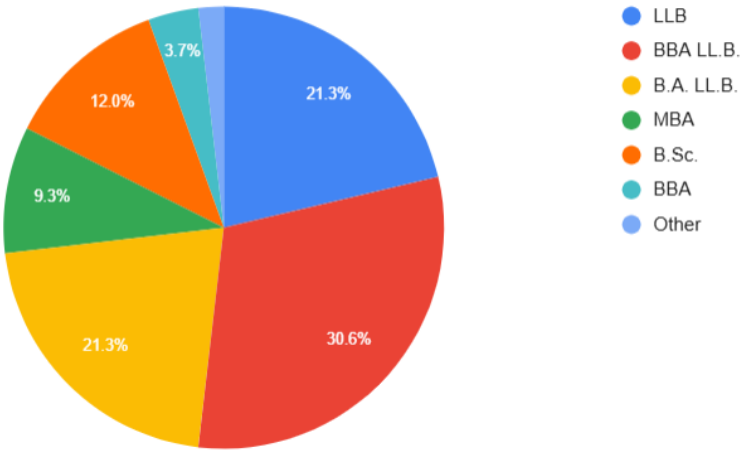






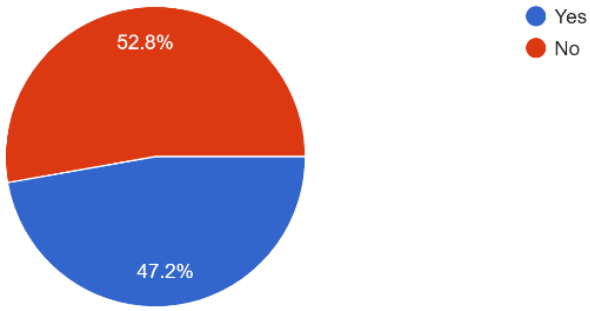
Course Pursuing

108 responses



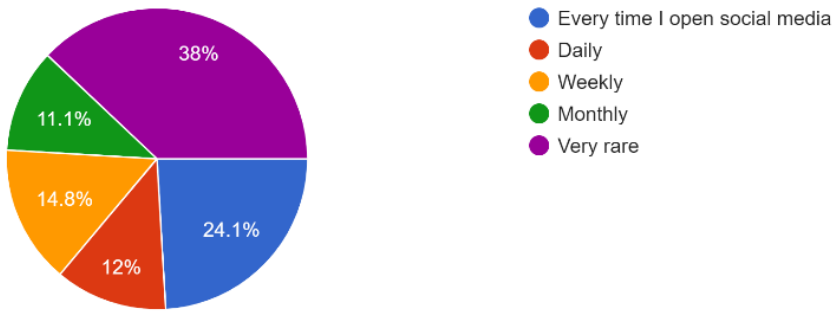
1. Have you personally encountered artificially manipulated face images or videos?

108 responses



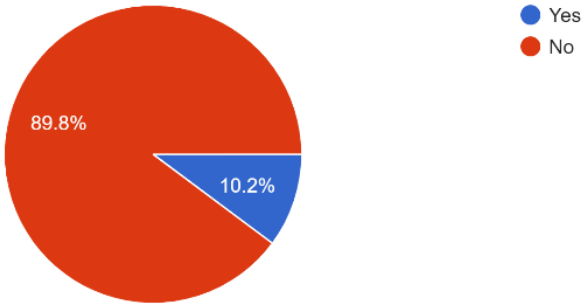
2. How often do you think you see an artificially manipulated image or picture?

108 responses



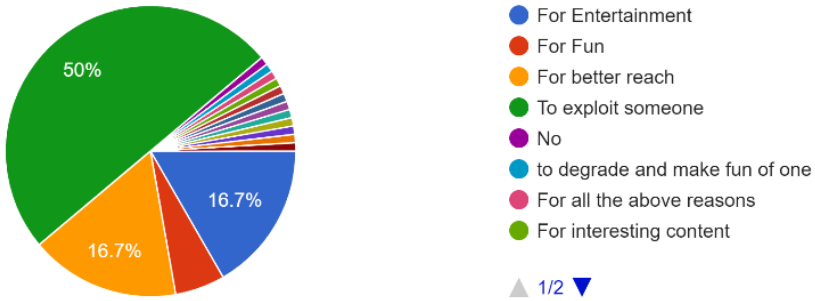
3. Have you manipulated or edited any such images/videos?

108 responses



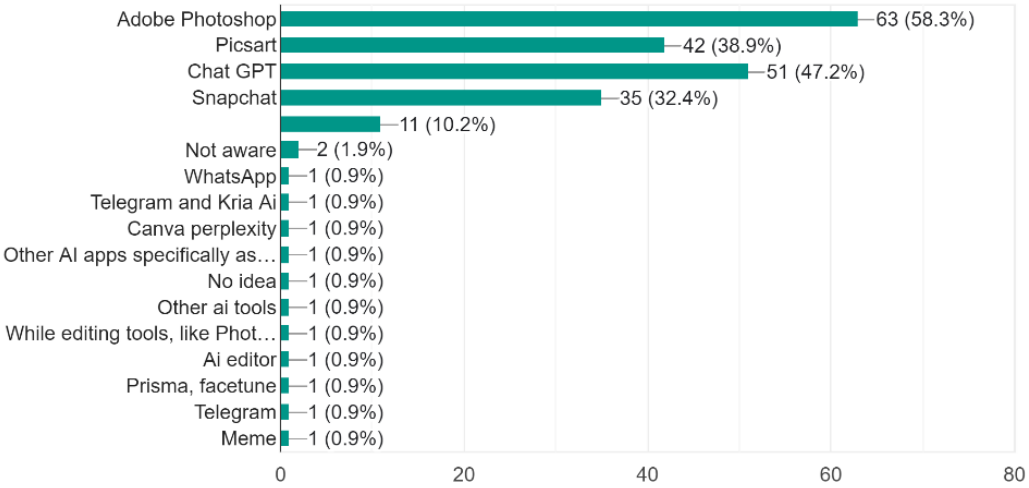
4. Why do you think they are created?

108 responses



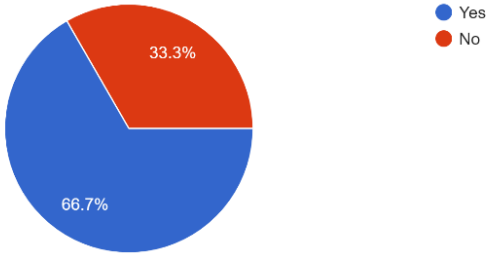
5. What are the different apps on which you are aware that AI generated content can be created?

108 responses



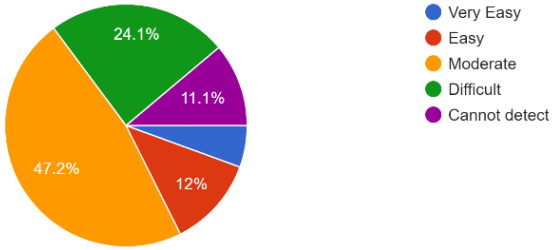
6. Have you heard of the terminology "deepfake"?

108 responses



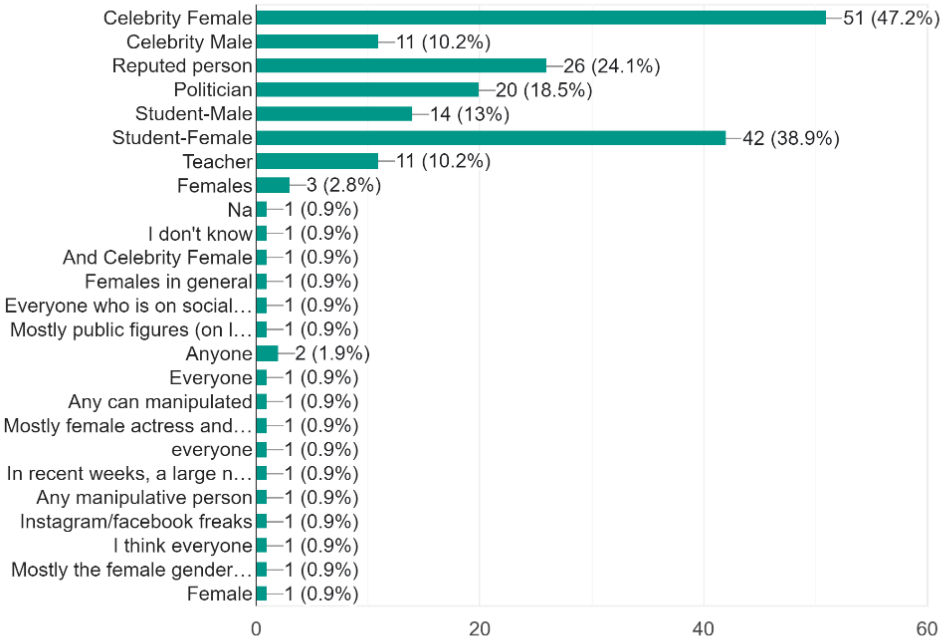
7. How difficult or easy is it to detect a deepfake?

108 responses



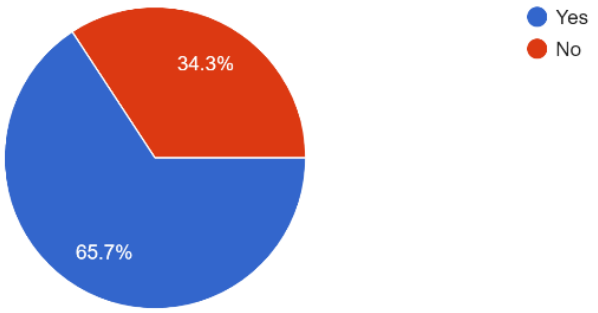
8. Who are most vulnerable to deepfake manipulation?

108 responses



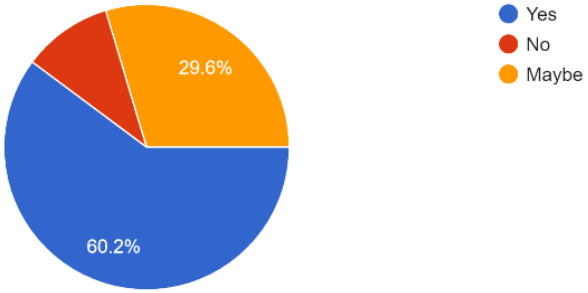
9. Are you ever worried about being a person on whom deepfake could be created?

108 responses



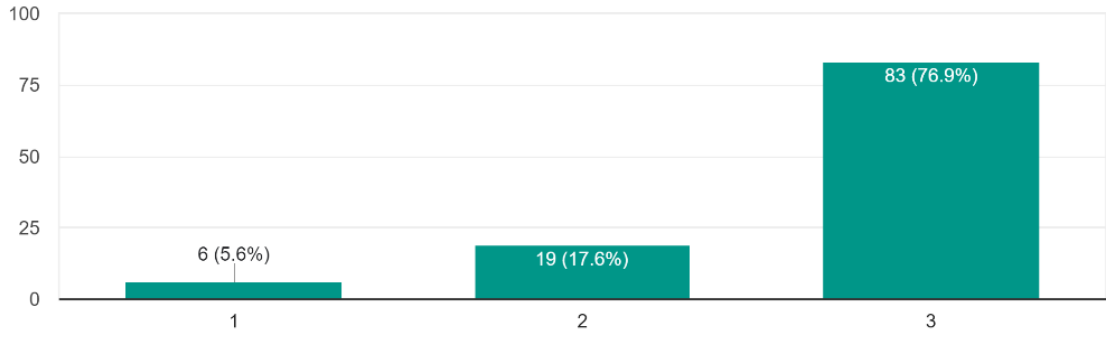
10. Do you believe that the widespread availability of mobile phones has made it easier for people to create and distribute deepfakes?

108 responses

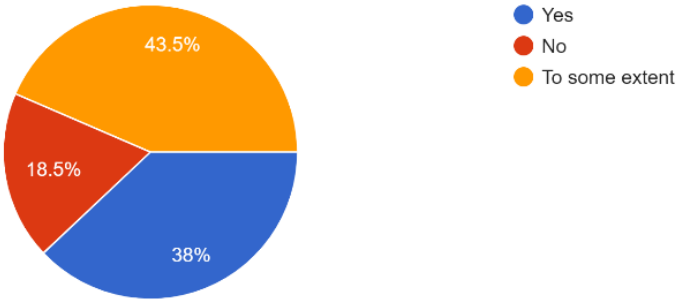


11. How harmful can using deepfake be for human beings?

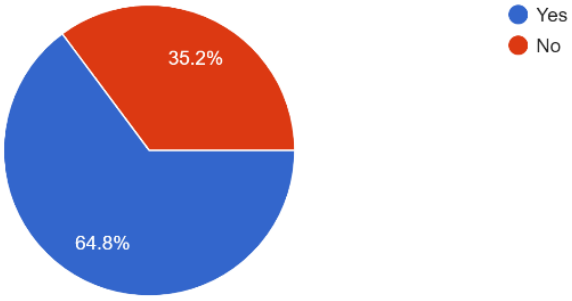
108 responses



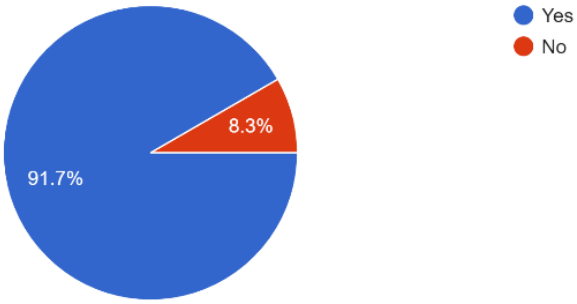
12. Has encountering a deepfake influenced your level of trust in digital media or information?
108 responses



13. Do you take any preventive action in day to day life to avoid misuse of your images through deepfake?
108 responses

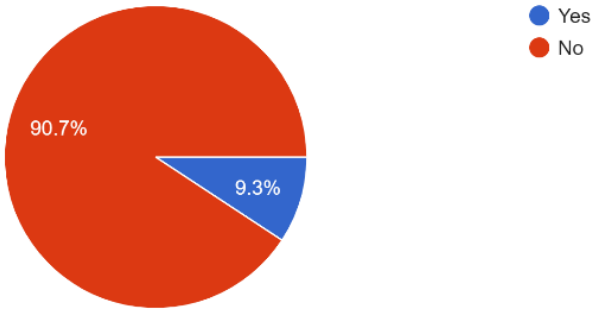


14. Do you believe that the creation of deepfake images can negatively impact a person's reputation or well-being?
108 responses



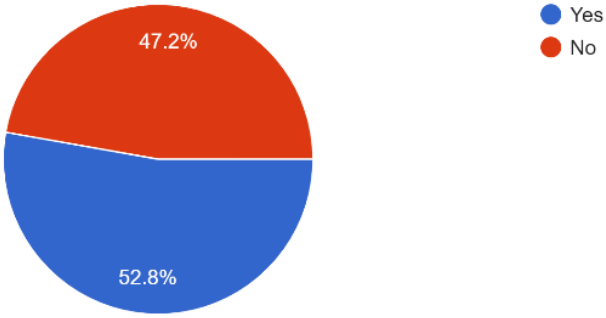
15. Have you ever been a target of deepfake?

108 responses



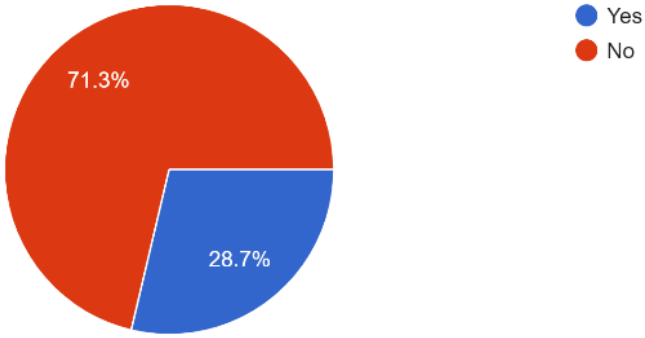
16. Do you know anyone who have been a target?

108 responses



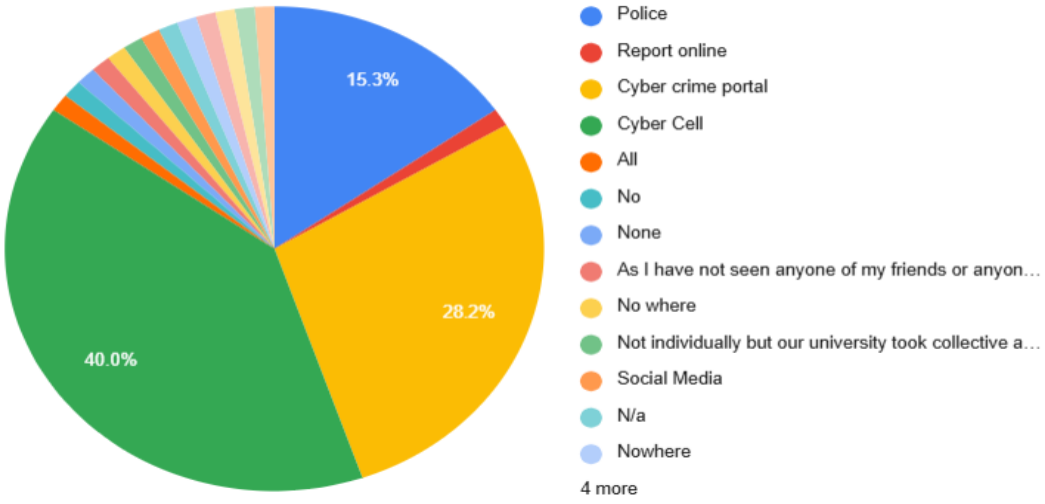
17. Have you raised a complaint regarding such issues?

108 responses



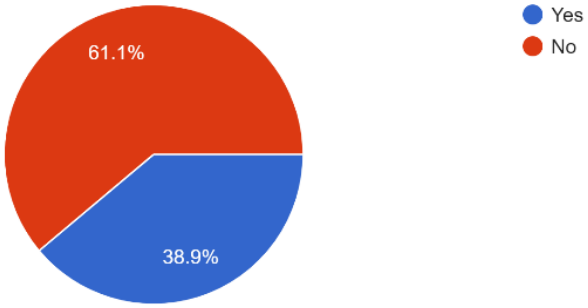
18. Where did you raise such complaints?

91 responses



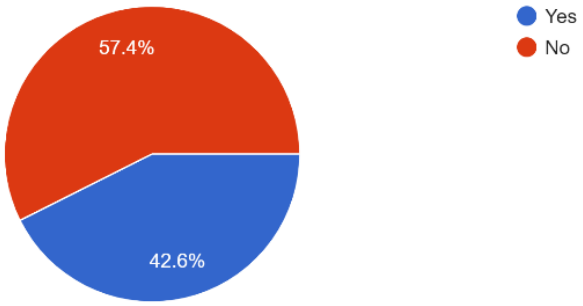
19. Did any police officer or investigation agency help you?

90 responses



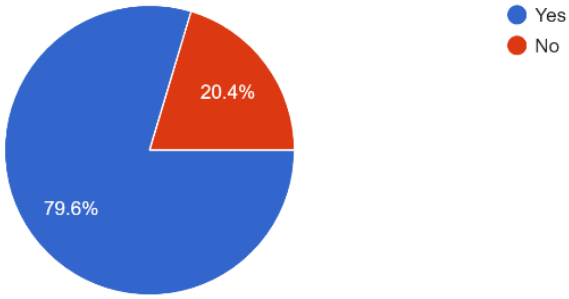
20. Are you aware of the minimum rank of police officer who would typically investigate a complaint related to deepfake content?

108 responses



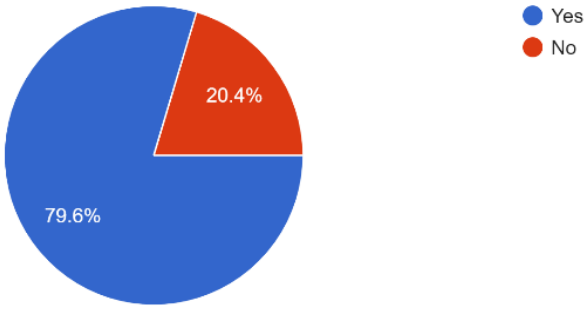
21. Are you aware that it is possible to file an FIR (First Information Report) against the creation or distribution of deepfake content?

108 responses



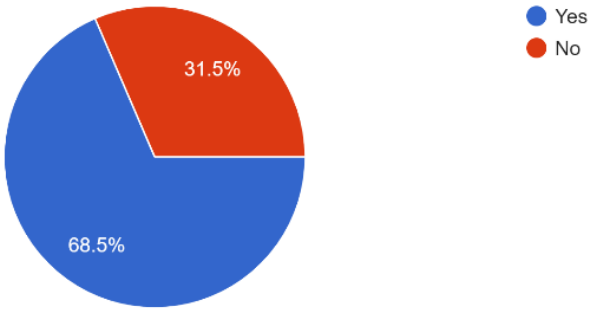
22. Do you know that the cyber cell is established in every district to help with these complaints?

108 responses



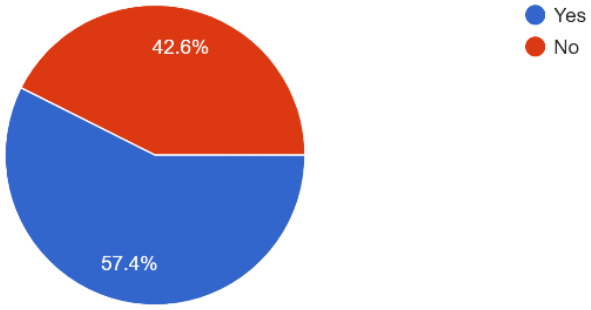
23. Are you aware that it's possible to seek compensation for injuries or defamation caused by deepfakes?

108 responses



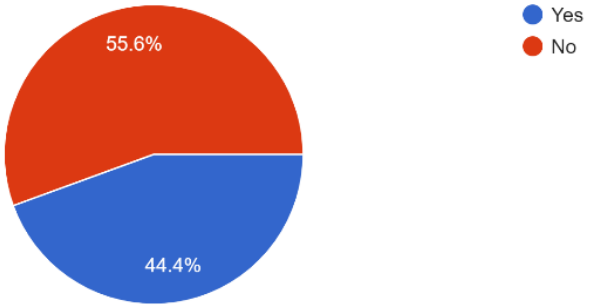
24. Are you familiar with specific laws in India that aim to protect individuals or organizations from the harmful effects of deepfakes?

108 responses



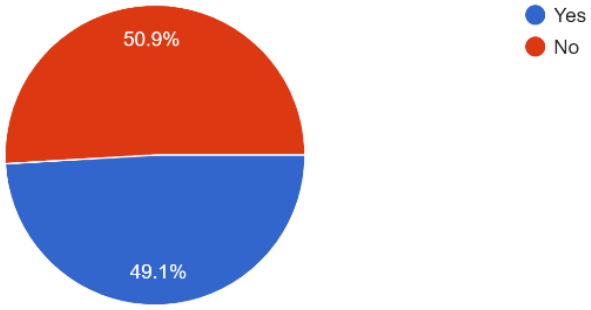
25. Are you aware of different government regulations which provide protection from deepfakes?

108 responses



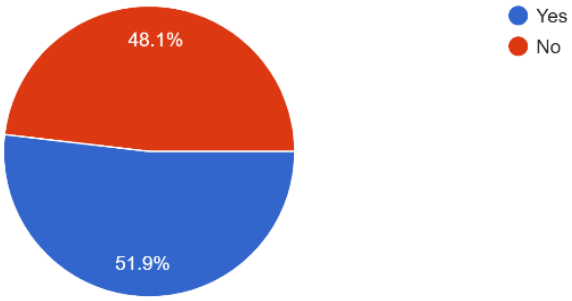
26. Are you familiar with the provisions of the Information Technology Act, 2000, as they relate to deepfakes?

108 responses



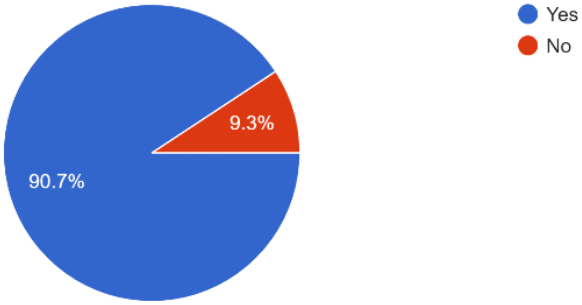
27. Are you aware of any regulations or guidelines that require social media platforms or other intermediaries in India to remove deepfake content within 36 hours?

108 responses



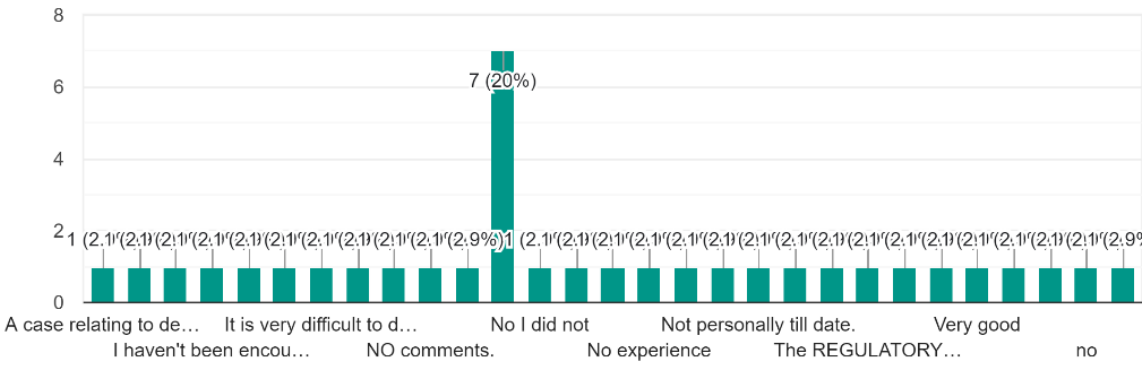
28. Do you think that there is a need for more stringent and specific laws to deal with deepfake incidents in India?

108 responses



If you have encountered any issues related to deepfakes, please share your experiences or thoughts

35 responses



8. CONCLUSION

With the advancement in technology, it is of pivotal importance that Legislators and Regulatory Authorities act with haste in strengthening laws and regulations relating to deepfakes to create safeguards for potential harms by balancing innovation and advancement in technology. Creating awareness for such safe guards among people is of dire need in today's world. As per the current study's analysis shows that majority of deepfakes are created to exploit someone with females being most vulnerable to being targeted be it a celebrity or student, 91% of individuals agree that deepfakes can negatively impact a person's reputation and wellbeing. Deepfakes have influenced people's trust in digital media and information there is still a gap of knowledge among today's youth regarding the laws and the government authorities who provide help regarding such incidents which according to data collected was 50% of individuals. 60% of individuals reported that no help was offered when the encountered such incident and majority of them did not ask for help in the first place. Almost 90% of our study participants agree that there is a need for more stringent safeguards for deepfake technology. 57.4% subjects were not familiar with the specific laws in India that aim to protect individuals or organizations from the harmful effects of deepfakes. 31% did not know that compensation can be sought for injuries or defamation caused by deepfakes. 55.5% were not aware of the government regulations providing protection from deepfakes, 50.92% said they were not familiar with the Information Technology Act, 2000 which relates to deep fakes and 48.14% did not even know that there are guidelines that require social media platforms or other intermediaries in India to remove deepfake content within 36 hours.