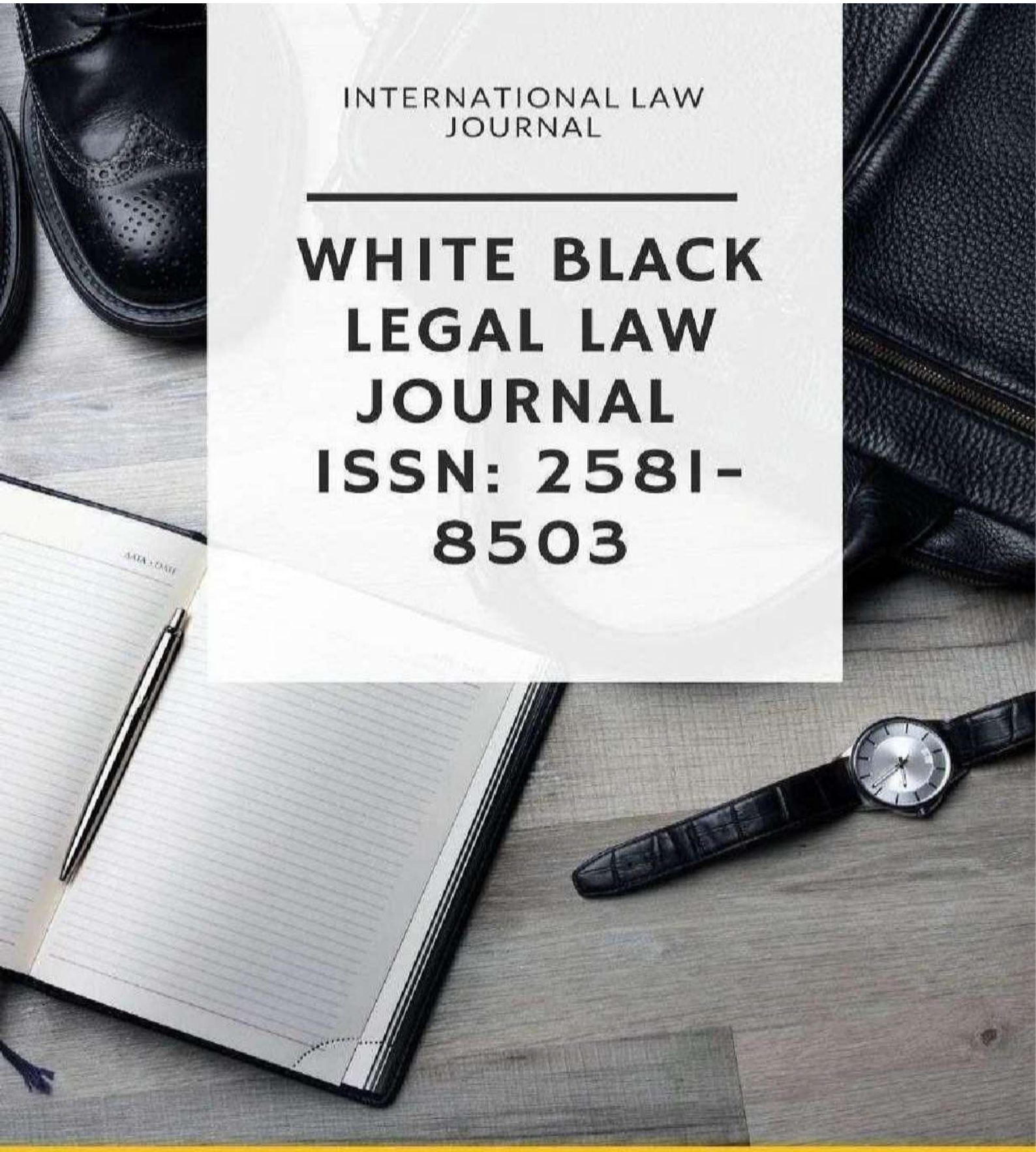

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

DEEPFAKES UNMASKED: DECODING INDIA'S LEGAL LANDSCAPE. DEMOCRACY AT RISK, PRIVACY UNDER SIEGE, CELEBRITIES IN DISTRESS

Sub-theme: The Evolving Legal Landscape: Navigating Technology's Impact

AUTHORED BY: SHASHANK SATISH MADYASTHA

Contact Number: 9741443055

Email Id: shashankoa@gmail.com

Abstract:

Originating on Reddit in 2017, the term 'deepfake' has evolved into a growing menace, plaguing society with instances of sextortion[1], blackmail, identity theft, and disinformation. This research employs trusted literature from journals, newspaper articles, and blogs to delve into the true extent of the deepfake threat. Results reveal that the deepfake technology, despite having some positive uses , causes adverse impact on democracy, privacy, consumer trust, and personality rights[2].

The paper unfolds in a three-section legal discussion: Firstly, it explores potential democratic implications, analyzing existing Indian legal safeguards, and proposing reforms inspired by global best practices. Secondly, it navigates the privacy landscape, the study engages in the 'right to be forgotten'debate, recommending tailored reforms in Indian law and drawing from international precedents. Thirdly, it scrutinizes the impact on personality rights, particularly in misleading ads, and advocates for reforms within the Indian legal framework. Finally, the paper concludes by proposing possible technological solutions to detect deepfakes, paving the way for a comprehensive defense against this menacing threat.

[1] In the report: Sextortion A crime of corruption and sexual exploitation, the defintion of the word sextortion is given. The international Association Of Women Judges have defined sextortion as "[A] form of sexual exploitation and corruption that occurs when people in positions of authority whether government officials, judges, educators, law enforcement personnel, or employers seek to extort sexual favours in exchange for something within their power to grant or withhold. In effect, sextortion is a form of corruption in which sex, rather than money, is the currency of the bribe." in IAWJ, *Twenty Five Years of Judging for Equality (2016) 179.*

[2] Personality rights, also known as the 'right of publicity,' acknowledge an individual's status as both a physical and spiritual being, ensuring their enjoyment of their own sense of existence. It encompasses various laws related to personality, and it grants individuals, particularly public figures or celebrities, the authority to manage and regulate the commercial use of their identity.

Keywords: 'Deepfake', 'Democracy', 'Privacy rights', 'Right to be Forgotten', 'Personality rights', 'misleading ads'.

Introduction:

There are numerous definitions of democracy, but the one given by Abraham Licon - "Government of the people, by the people, for the people."[3], by far outshines the others, being a comprehensive definition, as apart from a type political system, it also envisions democracy as a government which works for the people. The Indian democracy, is one such which stands tall and true to this definition, evident by the improvement of the condition of the people by public policy measures such as: land redistribution, subsidised food for the poor, reduction of absolute poverty.

Despite popular clamouring by the west of the impending doom of Indian democracy, Indian democracy has stood the test of time, overcoming numerous challenges such as - abrupt transitions of Prime Ministers[4], wars, intense communal conflicts. However, now the Indian democracy faces a new threat in the form of deepfake technology. Deepfake technology is used to spread fake news on social media, which negatively impacts the image of election candidates. This can lead to voters being unable to make free decisions on election day, which goes against their electoral rights. Deep-fake technology's threat to Indian democracy is not just limited to its effects on voters on election day but, also threatens to: erode the trust in democratic institutions, increase social divisions, etc.

One of the most prominent threats of Deep-fake technology on citizens' rights is that of privacy violations by use of deepfake technology, which not only invades the privacy of the person but also impacts the public image, dignity of the person concerned, especially in the case of pornographic content created using deepfake technology.

Another emerging misuse of the technology involves creating ads using the likeness of actors without their consent, thereby leveraging the fan base of these actors to generate revenue. This utilization of technology presents a dual-fold legal issue. Firstly, it raises concerns about not obtaining the actors'

[3] This famous phrase was given by Lincoln in his Gettsysburg Address on 19th November 1863 in the memory of the fallen soldiers who took part in the battle of Gettysburg during the American Civil War

[4] Regime change due to death of Jawaharla Nehru, Assassinations of Indira Gandhi and Rajiv Gndhi

consent before featuring their likeness in ads. Secondly, it gives rise to the problem of misleading consumers by falsely implying that certain celebrities have endorsed the ads.

This paper is structured into four distinct sections. The first part introduces Deepfake technology and elucidates its fundamental mechanisms. The second part explores the positive applications of Deepfake technology. The third part delves into the negative implications of Deepfake technology, addressing its threats to democracy, privacy, and personality rights. This section critically analyzes existing Indian laws, proposes amendments, and draws insights from global legal perspectives. The final part focuses on recommendations for the adoption of various technologies to bolster India's capabilities in detecting and countering Deep-fake.

Research Objective:

Investigate the multifaceted threats arising from the application of deep-fake technology on democracy, privacy, and personality rights in India. Evaluate the efficacy of existing legal provisions in India to counter these threats and offer recommendations based on global legislative practices to enhance regulatory frameworks.

Hypothesis:

This research posits that the widespread influence of deepfake technology presents intricate legal challenges, detrimentally affecting democracy, privacy, and personality rights.

Research Methodology:

This research employs a diverse range of secondary sources, such as reputable journals, legal reports, respected newspapers, and online legal portals. The methodology employs qualitative analysis for flexibility and adopts a deductive reasoning approach to refine formulated suppositions.

Discussion

I) Deep-Fake technology

In the framework discussed herein, a deepfake refers to the meticulous crafting of a video through sophisticated technological methods, presenting an individual engaged in speech or actions that they

never actually participated in. Deepfake videos typically utilize generative adversarial networks (GANs), a technology devised by Ian Goodfellow in 2014[5]. This GAN technology operates through a dynamic characterized by "mimics the back-and-forth between a picture forger and an art detective who repeatedly try to outwit one another."[6] In this process, the first network, referred to as the "generator," generates synthetic outputs until the second network, called the "discriminator," is unable to distinguish between the generator's outputs and an original dataset[7]. The outcome is a video with a convincingly realistic appearance. In essence, the technology takes an image, such as a face, comprehends it, and seamlessly incorporates it into a video, resulting in the substituted face blending seamlessly into the content.

The most effective approach to combat the issue of deepfakes is the establishment of a comprehensive legal framework that targets various participants throughout the deepfake lifecycle. The creation and dissemination of deepfakes involve multiple stages, and addressing this requires a systematic legal approach. The report "Tackling deepfakes in European policy"[8] offers a thorough set of policy options across various sectors, effectively addressing the deepfake phenomenon. The proposed legal framework is structured into five dimensions, corresponding to different stages in the deepfake lifecycle: technology, creation, circulation, target, and audience. These dimensions encompass policies targeting AI-based machine learning techniques, creators/users of AI systems, rules for deepfake dissemination, individual impacts on targets, and broader societal implications, respectively.

II) Positive Application of Deep-fake technology

Despite the contentious nature of the Deep-fake technology and its potential for nefarious purposes generating socially harmful results, Deep-fake technology has positive applications too, which used in the right way would result in greater social and individual benefits, especially in the case of education. Some of the positive applications of Deep-fake technology are:

[5]Martin Giles, The GANfather: The man who's given machines the gift of imagination, MIT Technology Review (Feb. 21, 2018), https://www.technologyreview.com/2018/02/21/145289/the-ganfather-the-man-whos-given-machines-the-gift-of-imagination/.
[6] Id
[7] Id
[8] Tackling deepfakes in European policy, European Parliament (July 30, 2021), https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039.

A. Education

Contrary to popular belief of the attention span being around 15 minutes[9], a study by Microsoft found that the average attention span of humans has now been decreased to 8s[10], which is in fact shorter than that of a goldfish. Studies[11] have shown that the use of videos in the lecutres can greatly enhance the learning process. The use of Deep-fake videos in education is similar to showing other educational videos, except for the Deep-fake videos being more compelling and thus retaining more attention. Through Deep-fake videos, it could be made possible to show historical figures speaking directly to the students[12], thus changing an otherwise, mundane lecture to an interesting one.

B. Art

The artistic use of Deep-Fake includes the educational use of it but not limited to it. There are numerous ways in which the Deep-Fake can be artistically used. For example, "Video artists might use deep-fake technology to satirize, parody, and critique public figures and public officials. Activists could use deep fakes to demonstrate their point in a way that words alone could not."[13] One of the emerging most popular artistic use of Deepfake technology, is the use of the previously created movies to generate a new movie, especially in the cases of dead actors, Rogue One released in 2016,[14] and Star Wars: The Last Jedi[15] being prominent examples.

C. Public Speaking

Public speaking, as a career, has been widely sought after by millions of people around the globe. The need for the skill is immensely important for almost all kinds of jobs[16], especially for aspiring diplomats, politicians, professional employee trainers in all companies, having a make/ break kind of

---

[9] Exeter, D.J., Ameratunga, S., Ratima, M., Morton, S., Dickson, M., Hsu, D. and Jackson, R., 2010. Student engagement in very large classes: The teachers' perspective. Studies in higher education, 35(7), pp.761-775.

[10] Kevin Mcspadden, You Now Have a Shorter Attention Span Than a Goldfish, Time (May 14, 2015), https://time.com/3858309/attention-spans-goldfish/.

[11](e.g., Allen and Smith, 2012; Kay, 2012; Lloyd and Robertson, 2012; Rackaway, 2012; Hsin and Cigas, 2013; Stockwell et al., 2015). - Cynthia J Brame & Kathryn E Perez, Effective Educational Videos: Principles and Guidelines for Maximizing Student Learning From Video Content, 15 CBE - Life Sciences Education (2017).

[12] Bobby Chesney & Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review 1753 (2019).

[13] Id

[14] Id

[15] Id

[16] Tim Smedley, Is public speaking fear limiting your career?, BBC (Mar. 22, 2017), https://www.bbc.com/worklife/article/20170321-is-public-speaking-fear-limiting-your-career.

effect on their career aspirations. Of the two new studies published by two computer scientists of University of Bath, UK, one of studies showcased Deep-Fake's capability in improving a person's public speaking skills[17]. This functions by substituting a user's face for that of a skilled public speaker, markedly enhancing the learning process. Confidence and perceived competence in public speaking increased substantially after viewing the FakeForward video. [18]

III) Negative Application of Deep-Fake technology

Despite the various positive applications of the Deep-fake technology, the potential outcome of the misuse of the technology greatly outweighs its benefits, from having extreme effects as threatening to weaken democracy to relatively minor ones such as satires, parodies on people having public posts.

A. Deepfake Implications on Indian Democracy:

The negative applications of Deep-fake technology either directly threaten democracy by threatening to manipulate the election results, thus directly affecting the implied electoral right of the voters to make a free decision or undermining democracy, deepfakes breed suspicion and discontent among citizens, eroding trust in democratic institutions.

i. Indian Elections:

The attention on the capability of deepfake to manipulate elections is heightened, especially with the general elections in 2024 being right around the corner. The government is actively countering the threat of deep-fakes, directing social media platforms to comply with IT rules19 amid concerns, especially as the 2024 general elections going to be one of the most important ones 20 so far, with state actors, and non-state actors alike keeping a close eye, looking to prevent the return of the incumbent PM Modi in 2024 due to political and geopolitical reasons.

The most terrifying example to date of foreign interference in the domestic elections of a country is

[17]Deepfake shows its positive face (2023) University of Bath. Available at: https://www.bath.ac.uk/announcements/deepfake-shows-its-positive-face/ (Accessed: 05 January 2024).
[18] Id
[19] Govt directs social media platforms to comply with it rules amid concerns over deepfakes (2023) The Indian Express. Available at: https://indianexpress.com/article/india/govt-social-media-platforms-it-rules-concerns-deepfakes-9083707/ (Accessed: 05 January 2024).
[20] G, M.C. (2024) Why 2024 could be among India's most consequential elections, The Indian Express. Available at: https://indianexpress.com/article/explained/explained-politics/looking-at-2024-politics-on-the-front-burner-in-an-election-year-9082634/ (Accessed: 05 January 2024).

that of Gabon, a country situated in West- Central Africa[21], faced an attempted coup due to the spread of the deep-fake video generated showing Gabon's president as sick which was used to suggest that he was unfit for the office. Foreign interference of this form has not occurred in India but has the potential to, given India's strained relations with its neighbours. The use of deepfake by non-state actors in influencing the elections is by far present and evergrowing[22] with notable examples such as 2020 Delhi assembly polls, Madhya Pradesh elections in 2023[23], thus a need to counter this menace.

Currently, specifically in respect to the use of deep-fake in elections, there exists the provisions within these acts: The Representation Of The People Act, 1951, The Bharatiya Nyaya (Second) Sanhita, 2023.

In respect to The Representation Of The People Act, 1951, sections 125 and section 126 are relevant to the use of deep-fake during elections.Section 125 criminalizes creating and spreading content to incite enmity between classes during elections. Its broad language suggests the inclusion of deepfake, as there is no specified restriction on how the information is disseminated. In respect to section 126, 126 (1) (b),(c) of the law can be interpreted to restrict the use of deepfakes during election campaigns. 126 (1)(b) prohibits displaying election-related content through cinematography, television, or similar devices in the 48 hours preceding the conclusion of a poll. 126 (1)(c) prohibits propagating election matter through activities like musical concerts or theatrical performances during this period. The term "election matter" broadly covers content intended to influence the election outcome, encompassing the potential use of deepfake technology for such purposes within the specified time-frame.

In respect to The Bharatiya Nyaya (Second) Sanhita, 2023, section 171 and section 356 are relevant to current discourse. While Deepfake technology can be presumed to apply to section 171, as the creation of fabricated content, including videos or audio recordings, aligns with provisions that

[21] Cahlan, S. (2020) How misinformation helped spark an attempted coup in Gabon. Available at: https://www.washingtonpost.com/politics/2020/02/13/how-sick-president-suspect-video-helped-sparked-an-attempted-coup-gabon/ (Accessed: 05 January 2024).

[22] Operation Deepfakes: India Today uncovers tech manipulators out to influence voters, polls (2023) India Today. Available at: https://www.indiatoday.in/india/video/operation-deepfakes-india-today-uncovers-tech-manipulators-out-to-influence-voters-polls-2480813-2023-12-26 (Accessed: 05 January 2024).

[23]Saha, B. and Tiwari, S. (2023) How deepfakes could impact Indian elections, India Today. Available at: https://www.indiatoday.in/elections/story/how-deepfakes-could-impact-indian-elections-2464241-2023-11-17 (Accessed: 05 January 2024).

consider threats or inducements aimed at candidates or voters as interference. Deepfakes can induce false beliefs, such as threats of divine displeasure, falling under the law's definition of interference with electoral rights. If used to mislead candidates or voters, deepfakes can be considered a form of undue influence, aligning with the law's intent to prevent coercion, inducement, or misinformation that hinders the free and fair exercise of electoral rights. On the other hand the deefake videos falls within the ambit of the section 356 and is currently the most relevant section to combat political deepfakes.[24]

One of the fundamental flaws of the laws regulating deep-fake elections is the low probability of punishment[25]. In respect to The Representation Of The People Act, 1951, while the section 125 does address the use of deep-fake technology to promote enemity of classes, the term of imprisonment for its violation is a mere 3 years, furthermore its limited to the prevention of 'enemity' between classes and does not address aspects of political deepfakes like character assassination. On the other hand, section 126 is largely redundant, due to the exclusion of propagation of deep-fake campaigns on social media, given the number of social media users in India[26]. With respect to sections 171, 356 of The Bharatiya Nyaya (Second) Sanhita, 2023, section 171 remains silent on satirical videos, which, by mocking aspects of a politician's policies or personal life, have the potential to alienate voters, with the intention of affecting the electoral right being absent. It could influence the perception of the politician, which could extend to creating false narratives around policies, character traits, potentially leading to reputational harm and impacting the electoral process.

While the most prominent legislations around the globe are EU's recent AI act, China's Administrative Provisions on Deep Synthesis of Internet Information Services (the "Provisions") and finally individual US state legislations on the use of deepfake technology during election, of which Californis's legislation being the most prominent one. Due to the Eu's AI act focusing mainly on an overarching AI framework with no comprehensive on regulating Deepfake[27], it cannot be used in this

[24] Section 356 language is broad enough to include deepfake videos also, give a short explanation
[25] Due to low technical ablities to detect deep-fakes accompanied by the democratisation of the technology, everybody having access to it.
[26] Dr. A. Shaji George (2023) "Regulating Deepfakes to Protect Indian Elections", Partners Universal Innovative Research Publication, 1(2), pp. 75–92. doi: 10.5281/zenodo.10154619.
[27] 19)Yinuo Geng*CITE AS: 7 GEO. L. TECH. REv. 157 (2023) - Geng, Y. (2023) Comparing 'deepfake' regulatory regimes in the United States, the European Union, and China, Georgetown Law Technology Review. Available at:

particular instance. However, the combination of California's law[28] and China's Provisions on deepfake synthesis offers a comprehensive and nuanced framework for regulating deepfake technology. California's law focuses on disclosure requirements[29], addressing manipulated audio or visual media through explicit statements and mandatory markings[30]. It incorporates measures for identity authentication, content control, and the handling of deceptive media while also fairly providing exceptions to the law[31]. China's Provisions take a broader approach, encompassing a vertical regulatory model with obligations for deep synthesis services providers, technology supporters, and services users. The "three-step method" in the Provisions aids enterprises in determining their regulatory status, emphasizing identity authentication, content control, and security measures.[32] While California's law emphasizes transparency and accountability in media manipulation, China's Provisions cover a spectrum of obligations for different entities involved in deep synthesis services.[33] Adopting elements from both could provide India with a comprehensive regulatory framework for addressing deepfakes during elections.

ii. Deepfake Impact on institutions and social divisions

Deepfake technology has played a significant role in eroding trust in democratic institutions and exacerbating social divisions in India. During the 2013 Muzaffarnagar communal riots, social media contributed to the dissemination of false information[34], such as an incendiary video funnelling communal divide[35]. The misuse of technology in spreading rumors during highlights the negative

https://georgetownlawtechreview.org/comparing-deepfake-regulatory-regimes-in-the-united-states-the-european-union-and-china/GLTR-01-2023/ (Accessed: 05 January 2024).

[28] Section 2010, division 20 of california election code

[29] Section 2010 (b) (1), (b) (2)

[30] Section 2010 (b) (3)

[31] Section 2010 (d) (2) (3) (4) (5), most prominent exceptions are broadcast made in goodfaith, with disclaimer of deepfake, publication of deepfake of general interest with disclaimer of it being a deepfake, deepfakes that constitute satire or parody.

[32] Peng, C. (2022) CAC issues landmark rule to rein in Deepfake Misuse, Lexology. Available at: https://www.lexology.com/library/detail.aspx?g=a8dda00e-1f3b-4c99-a098-2a9e395d8c65 (Accessed: 05 January 2024).

[33] id

[34] Jayanta Deka / TNN / Updated: Sep 10, 2013 (no date) Muzaffarnagar riots: On Social Media, rumours and Anger: India News - Times of India, The Times of India. Available at: https://timesofindia.indiatimes.com/india/Muzaffarnagar-riots-On-social-media-rumours-and-anger/articleshow/22446959.cms (Accessed: 05 January 2024).

[35] India Hunts 'Fake News' spreaders after anti-Muslim attacks (2021) The Guardian. Available at: https://www.theguardian.com/world/2021/nov/07/india-hunts-fake-news-spreaders-after-anti-muslim-attacks (Accessed: 05 January 2024).

impact on societal harmony and public trust in democratic processes[36]. WhatsApp, a widely used platform in India, has become a conduit for the rapid spread of rumors, contributing to incidents like lynchings[37]. The platform's role in circulating misinformation has been noted in events such as the 'Northeastern exodus' in 2012, subsequent lynchings from 2014 onwards.[38]

The problem is further exacerbated as diffusion of deep-fake technology is expected to occur rapidly and democratically, with the potential to be misused by various actors. The information cascade dynamic, human attraction to negative and novel information, and filter bubbles are identified as factors contributing to the viral spread of deep fakes. Negative and novel information tends to grab attention, leading to its rapid dissemination. The spread of false information is exacerbated by filter bubbles, which reinforce individuals' preexisting beliefs, creating powerful insulators against contrary information, eroding trust in democratic institutions and exacerbating social divisions.[39]

The new Bharatiya Nyaya (Second) Sanihita as well The IT Rules, 2021[40] together tackle the problem of deepfake with the former majorly focusing on the creators, distributors of the deepfake and the latter focusing on social media intemediatories and other media platforms. The issue of spreading fake news is addressed as a serious offense under both The Bharatiya Nyaya (Second) Sanhita, 2023, and the Information Technology Act, 2000. Relevant sections include 196, 197, 299, in the former, covering offenses promoting enmity, prejudicial imputations, outrage of religious feelings. The latter, under Section 3(1), imposes due diligence on intermediaries, requiring the publication of rules, privacy policies, and user agreements. It mandates prevention of hosting information violating norms, including spreading false information. Non-compliance leads to access termination, and cooperation with government agencies for investigation is mandatory, aiming to curb misinformation and maintain public order.

[36] Arun, C. and Nayak, N. (2016) Preliminary findings on online hate speech and the law in India, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2882238 (Accessed: 05 January 2024).
[37] Samuels, E. (2020) How misinformation on WhatsApp led to a mob killing in India. Available at: https://www.washingtonpost.com/politics/2020/02/21/how-misinformation-whatsapp-led-deathly-mob-lynching-india/ (Accessed: 05 January 2024).
[38] Arun, C. (2019) On WhatsApp, rumours, lynchings, and the Indian Government, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336127 (Accessed: 05 January 2024).
[39] See footnote 12
[40] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The legal framework introduced in the rules outlines additional due diligence measures for significant social media intermediaries to combat deepfake videos and ensure responsible content management.[41] Rule 7 emphasizes voluntary user verification mechanisms, and Rule 5 introduces additional due diligence for intermediaries handling news and current affairs content. These provisions collectively aim to enhance accountability, traceability, and transparency, focusing on safeguarding national interests and public order.

The proposed Digital Media Code of Ethics, alongside Michael Polányi's fiduciary program, forms a correlated strategy to combat deepfake videos. This comprehensive approach mandates ethical standards and introduces a three-tier self-regulating mechanism for news publishers and online platforms. Simultaneously, Polányi's program suggests branding reliable information, creating a trusted standard for online news[42]. This dual strategy accommodates diverse online content while ensuring reliability. Frequent audits of news agencies complement this, serving as a vital component to guarantee sustained credibility.

B. Deepfake Implications on Privacy:

Deepfake technology poses a significant threat to individual privacy in India, particularly with a focus on non-consensual deepfake pornography, as evidenced by several alarming incidents. The Bollywood industry has been shaken by deepfake controversies involving actresses such as Rashmika Mandanna, Alia Bhatt, Kajol, Aishwarya Rai, and Katrina Kaif. These incidents have sparked nationwide conversations about the ethical implications of deepfake technology, leading to arrests by the Delhi Police. The 2023 State of Deepfakes report[43] indicates a 550% increase in deepfake videos since 2019, with approximately 98% being pornographic and 99% targeting women, presenting a clear pattern of invasion of privacy.[44] Furthermore, the rise of 'sextortionists' in India, using deepfake

[41] Rule 4(1) mandates the appointment of a Chief Compliance Officer, a nodal contact person for 24x7 coordination with law enforcement, and a Resident Grievance Officer. Rule 4(2) requires enabling the identification of the first originator of information.

[42] Ziegler, Z., 2023. Michael polányi's fiduciary program against fake news and deepfake in the digital age. AI & SOCIETY, 38(5), pp.1949-1957.

[43] Standard, B. (2023) AI-powered deepfakes rise in 2023; concerns of its impact on privacy, Business Standard. Available at: https://www.business-standard.com/technology/tech-news/ai-powered-deepfakes-rise-in-2023-concerns-of-its-impact-on-privacy-123123100076_1.html (Accessed: 05 January 2024).

[44] Aakash Sharma, Bollywood to war: How the year of deepfakes unfolded, India Today (Dec. 22, 2023), https://www.indiatoday.in/india/story/deepfake-artificial-intelligence-cyber-crime-elections-bollywood-actors-digital-world-2479431-2023-12-22.

sexual videos to blackmail and extort money from Bollywood celebrities and other prominent individuals, underscores the gravity of the issue. Such criminals exploit the vulnerability of individuals through morphing faces into objectionable multimedia clips, causing significant psychological and financial harm.[45]

The impact of non-consensual deepfake pornography on female journalists has also been documented, revealing the severe emotional and professional consequences. The Power and Control Wheel tactics, facilitated by apps like FaceApp, have made it increasingly easier for individuals to create deepfake pornography without consent, endangering victims like journalist Rana Ayyub[46], who faced a deepfake campaign aimed at silencing her advocacy. The emergence of unethical platforms, such as the unnamed service described in MIT Technology Review, allows users to turn anyone into a porn star by swapping faces into adult videos with just a photo upload[47]. This ease of use raises concerns about the potential widespread misuse of deepfake technology. The consequences for women and girls targeted by such activities are devastating, akin to revenge porn, causing severe psychological trauma and violating their identity, reputation, and privacy. These instances highlight the urgent need for robust legal measures and increased awareness to counter the growing threat of deepfake-related privacy breaches in India.

The legal landscape in India that governs the privacy of individuals and addresses the specific challenges posed by deepfake technology, particularly in the context of deepfake pornography, is comprehensive and multifaceted. The Digital Personal Data Protection Act, 2023, establishes a robust framework by defining crucial terms, such as "Data Fiduciary" and "Data Principal," and ensuring lawful processing of personal data. Sections 4, 7, and 8 lay down principles for processing personal data, including security safeguards, and highlight permissible uses of data related to deepfake technology. Section 9 specifically addresses children's personal data, emphasizing verifiable consent. The Act enhances transparency with Section 11, granting Data Principals the right to access information about their data processing, a crucial aspect in the context of deepfake activities. Sections

[45] Narayan Namboodiri, Deepfake clips: 'Sextortionists' target celebs, Times of India (Feb. 23, 2021), https://timesofindia.indiatimes.com/city/mumbai/deepfake-clips-sextortionists-target-celebs/articleshow/81162493.cms.
[46] Journalist Rana Ayyub Is Fighting to Expose the Truth in India, TIME (Oct. 22, 2021), https://time.com/6108251/rana-ayyub-india-journalism-modi/.
[47] Karen Hao, A horrifying new AI app swaps women into porn videos with a click, MIT Technology Review (Sept. 13, 2021), https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/.

14 and 15 provide safeguards, allowing Data Principals to nominate representatives and outlining their duties, thus mitigating privacy risks arising from deepfake, including the potential for misuse.

In parallel, the IT Rules, 2021 as amended in 2023, complement these efforts by addressing privacy challenges associated with deepfake technology. Section 3(1) imposes due diligence obligations on intermediaries, necessitating the publication of rules, regulations, and privacy policies. Section 4 emphasizes the prevention of hosting obscene or pornographic content, aligning with concerns related to deepfake pornography. The provision in Section 4(2)(j) ensures prompt provision of information to lawful authorities. Simultaneously, the Information Technology Act, 2000, under Sections 66E, 67, 67A, and 67B, criminalizes the capture, publication, or transmission of private images without consent and the dissemination of obscene or sexually explicit material, providing a strong legal stance against such activities. The POCSO Act, in Sections 13, 14, and 15, further strengthens this framework by penalizing the use of children for pornographic purposes.

In the intricate web of Indian legal frameworks designed to combat the privacy implications of deepfake, significant gaps persist despite the existence of crucial laws such as The Digital Personal Data Protection Act, 2023; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Information Technology Act, 2000; and The POCSO Act. Notably, The POCSO Act addresses the use of technology for producing child pornography, but this protective umbrella is narrowly cast and does not extend to the broader populace. The proliferation of emerging apps like FaceApp and those spotlighted by the MIT Review poses an imminent threat to the efforts in curbing deepfake circulation, given the widespread accessibility of deepfake technology. To confront this challenge head-on, there's a pressing need to bolster preventative measures and criminalize the harmful applications of such technology. Establishing an enforcement body akin to the European Artificial Intelligence Board (EAIB) under the EU AI Act becomes paramount to effectively regulate emerging technologies, ensuring their responsible development for the benefit of human life. In India, current legislative acts primarily concentrate on the role of social media intermediaries and their efforts to mitigate immoral content, with limited provisions dedicated to addressing deepfake-related privacy concerns at large.

A shining beacon in this legal landscape is the concept of the "right to be forgotten," akin to Article

17 of the EU's General Data Protection Regulation. This right empowers individuals to request the erasure of personal data under specific circumstances, presenting a balanced approach that prevents censorship while safeguarding freedom of speech. The right to be forgotten has found roots in Indian law, notably in Section 72 of The Bharatiya Nyaya (Second) Sanhita, 2023. However, its application is currently limited to victims of rape. It lays a foundational precedent for addressing privacy concerns in the digital realm, especially concerning the misuse of personal data. Legal judgments, including the watershed moment in the Justice KS Puttaswamy case, recognized the fundamental right to privacy in India. A more recent and impactful example is the case of X v YouTube. In this case, the plaintiff, a prominent actor in the Indian Film Industry, sought the removal of videos containing explicit content that were edited and released without her consent on various online platforms. The Delhi High Court acknowledged the plaintiff's right to privacy and invoked the right to be forgotten, ordering the prompt removal of all videos within 36 hours. This landmark decision reinforces the importance of protecting individuals from the deleterious effects of deepfake pornography, establishing a significant precedent for future cases.

C. Deepfake and Personality Rights:

The US Court of Appeals for the Second Circuit, in Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., elucidated the essence of personality rights, emphasizing the protection of the publicity value of one's photograph. The case highlighted that prominent individuals would feel deprived if not compensated for authorizing advertisements, and unauthorized publicity would lack financial benefits without an exclusive grant. The evolution of intellectual property protection began with the Paris Convention, addressing inventors' concerns. Subsequently, the TRIPS agreement in 1995 extended protections to various intellectual property fields. Shrimati Shantabai v. State of Bombay & Others clarified intellectual property as a form of property, grounded in natural rights advocated by philosophers Locke and Kant. The Personality Rights theory justifies creators' natural rights to express their creative work, emphasizing protection based on personality over purely monetary considerations. This theory safeguards the creator's unique connection to the creation, asserting rights over the result of their invested labor. Focused on protecting personality interests, it posits that creators should have the right to protect aspects of their personality in their creations. In India, unauthorized commercial use of celebrities' names and images, as seen with Virat Kohli, P.V. Sindhu, and Shashi Tharoor, necessitates legal protection of personality or celebrity rights.

In India, the legal landscape regarding Personality Rights is evolving, lacking a separate codification. The common law right of publicity safeguards a notable person's ownership interest in the financial success of their public reputation or image. While not explicitly recognized as individual rights, Personality Rights encompass publicity and privacy rights, with Article 21 of the Indian Constitution, the Right to Life, being a dominant provision governing these rights. Publicity rights prevent unauthorized commercial exploitation of a person's name or image, while privacy rights allow individuals to be left alone, barring the reflection of their personality in public without consent. Though not expressly stated in Article 21, the courts, including the Supreme Court, have interpreted fundamental rights, including publicity and privacy rights. The judiciary, in cases like RajaGopal and Shivaji Rao Gaikwad, emphasized protection against unauthorized use. Judicial pronouncements, as seen in ICC Development and Titan Industries cases, stress the importance of attention rights as inherent in a person's identity characteristics. However, the transferability of personality rights after death was clarified in Deepa Jayakumar v. AL Vijay, stating that such rights do not endure beyond an individual's life.

The Copyright Act, while posing challenges in recognizing Personality Rights, protects certain aspects under Section 38 and 38A, with the case of Tanishq illustrating ownership based on agreements. Trademarks Act 1999 provides limited protection through Section 14, prohibiting the use of individual names falsely suggesting an association with a living person. The Consumer Protection Act 2019 addresses misleading advertisements, empowering authorities to take action against violators. Notably, recent cases involving Amitabh Bachchan and Anil Kapoor showcase the judiciary's proactive stance in protecting personality rights in the context of technological advancements like deepfake videos. The Delhi High Court's decisions, especially in Anil Kapoor's case, underscore the need for comprehensive legislation explicitly recognizing personality rights as distinctive intellectual property, allowing for commercial licensing, economic benefits, and protecting individuals from unauthorized and illegal use of their persona. Such legislation would also contribute to public awareness and education about the significance of personality rights and responsible marketing practices.

The recent U.S. bill, known as the "NO FAKES Act of 2023," offers a comprehensive framework that can serve as a valuable reference for shaping future Indian legislation aimed at safeguarding

personality rights from deepfake technology infringement. The bill defines key terms such as "digital replica," "individual," "sound recording artist," and "visual likeness," providing clarity on the scope of protection. It establishes a digital replication right, emphasizing its property nature, inheritability, and exclusivity, even beyond an individual's death. The liability section holds individuals engaging in unauthorized digital replica activities accountable, ensuring civil actions for damages sustained by the affected party. The bill's exclusions, addressing news, documentaries, satire, and de minimis use, strike a balance between protecting rights and preserving freedom of expression. The civil action provisions specify eligible plaintiffs, limitations period, defenses, and remedies, including punitive damages. Importantly, the bill emphasizes non-preemption of other protective laws and is constructed as pertaining to intellectual property. This legal framework, addressing emerging challenges posed by deepfake technology, provides a robust foundation for India to enact legislation ensuring equitable protection of personality rights while promoting freedom and expression.

IV) Deepfake Detection:

In India's dynamic landscape, the relentless evolution of deepfake technology poses a formidable challenge, demanding an adaptable approach to detection. Deep learning algorithms, particularly deep neural networks, emerge as a frontline defense, discerning patterns and anomalies in vast datasets of real and fake media. By training these algorithms to recognize subtle visual artifacts and inconsistencies like unnatural facial movements or audio-visual mismatches, they become adept at flagging potential manipulations for further scrutiny.

Visual artifacts, the fingerprints of deepfakes, offer crucial cues. Unnatural facial expressions, erratic eye blinking, and incongruities in the background serve as red flags. Forensic-based methods, scrutinizing geometric relationships and visual cues, add an extra layer of inspection. Yet, acknowledging their fallibility is vital, as deepfake creators continually refine their techniques, demanding constant updates to detection methods. A pivotal strategy in fortifying deepfake detection involves the synergy of various detection methods through multi-model ensembles. Microsoft's innovative tool, assigning confidence scores to media authenticity, exemplifies this approach. In anticipation of deepfake technology's rapid evolution, Microsoft's collaboration with media organizations on Project Origin introduces a groundbreaking concept—marking online content with a digital fingerprint, a formidable weapon against disinformation.

In the face of a scenario where deepfake videos erode public trust in news across India, particularly in the absence of a perceived reliable central authority, the adoption of distributed ledger technologies (DLTs) and blockchain becomes imperative. These technologies offer decentralized solutions, ensuring traceability, privacy, and security. DLTs control the traceability of media, communications, and transactions, presenting a robust solution to the challenges posed by fake news and deepfakes. Blockchain applications, ranging from decentralized content moderation and fact-checking incentivized dApps to notarization services and traceability mechanisms, collectively compose a comprehensive strategy. However, a nuanced understanding of DLT-based solutions is paramount, considering optimization for specific use cases, cybersecurity, compliance with data protection regulations, and the ongoing need for collaborative efforts. The integration of DLTs with AI and NLP methods holds promise, offering profound insights to combat digital deception effectively. As the landscape of deepfake technology evolves, persistent research and collaborative endeavors remain indispensable to cultivate resilient strategies against its advancing capabilities.

Conclusion:

While there are various positive applications of deep-fake technology as explored in the form of education, art, public speaking, the potential for misuse of the technology and its eventual impact on democracy, privacy, personality rights necessitates the responsible management of the technology by a combined techno - legal operations to prevent its abuse. While there are provisions related to addressing these challenges in our legal system, they however, by themselves, do not suffice, as they have not been amended to reflect the current scenario, especially in the case of law relating to elections and personality rights. While the privacy laws are relatively well developed, they are not all inclusive with room for improvement. Refernce to prominent global legislations can be made to incorporate some of the features which are best suited to the Indian legal landscape. However, on a positive note, the capability of these deepfake systems/apps to cause chaos and instability has been duly noted by the government, as is evident with the IT minister's announcement of new regulations to combat the spread of deepfakes on social media platforms.

References:

1) Martin Giles, The GANfather: The man who's given machines the gift of imagination, MIT Technology Review (Feb. 21, 2018), https://www.technologyreview.com/2018/02/21/145289/the-ganfather-the-man-whos-given-machines-the-gift-of-imagination/.

2) Tackling deepfakes in European policy, European Parliament (July 30, 2021), https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039.

3) Exeter, D.J., Ameratunga, S., Ratima, M., Morton, S., Dickson, M., Hsu, D. and Jackson, R., 2010. Student engagement in very large classes: The teachers' perspective. Studies in higher education, 35(7), pp.761-775.

4) Kevin Mcspadden, You Now Have a Shorter Attention Span Than a Goldfish, Time (May 14, 2015), https://time.com/3858309/attention-spans-goldfish/.

5) Cynthia J Brame & Kathryn E Perez, Effective Educational Videos: Principles and Guidelines for Maximizing Student Learning From Video Content, 15 CBE - Life Sciences Education (2017).

6) Bobby Chesney & Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review 1753 (2019).

7) Tim Smedley, Is public speaking fear limiting your career?, BBC (Mar. 22, 2017), https://www.bbc.com/worklife/article/20170321-is-public-speaking-fear-limiting-your-career.

8) Deepfake shows its positive face (2023) University of Bath. Available at: https://www.bath.ac.uk/announcements/deepfake-shows-its-positive-face/ (Accessed: 05 January 2024).

9) Govt directs social media platforms to comply with it rules amid concerns over deepfakes (2023) The Indian Express. Available at: https://indianexpress.com/article/india/govt-social-media-platforms-it-rules-concerns-deepfakes-9083707/ (Accessed: 05 January 2024).

10) G, M.C. (2024) Why 2024 could be among India's most consequential elections, The Indian Express. Available at: https://indianexpress.com/article/explained/explained-politics/looking-at-2024-politics-on-the-front-burner-in-an-election-year-9082634/ (Accessed: 05 January 2024).

11) Cahlan, S. (2020) How misinformation helped spark an attempted coup in Gabon. Available at: https://www.washingtonpost.com/politics/2020/02/13/how-sick-president-suspect-video-helped-sparked-an-attempted-coup-gabon/ (Accessed: 05 January 2024).

12) Operation Deepfakes: India Today uncovers tech manipulators out to influence voters, polls (2023) India Today. Available at: https://www.indiatoday.in/india/video/operation-deepfakes-india-today-uncovers-tech-manipulators-out-to-influence-voters-polls-2480813-2023-12-26 (Accessed: 05 January 2024).

13) Saha, B. and Tiwari, S. (2023) How deepfakes could impact Indian elections, India Today. Available at: https://www.indiatoday.in/elections/story/how-deepfakes-could-impact-indian-elections-2464241-2023-11-17 (Accessed: 05 January 2024).

14) Dr. A. Shaji George (2023) "Regulating Deepfakes to Protect Indian Elections", Partners Universal Innovative Research Publication, 1(2), pp. 75–92. doi: 10.5281/zenodo.10154619.

15) Geng, Y. (2023) Comparing 'deepfake' regulatory regimes in the United States, the European Union, and China, Georgetown Law Technology Review. Available at: https://georgetownlawtechreview.org/comparing-deepfake-regulatory-regimes-in-the-united-states-the-european-union-and-china/GLTR-01-2023/ (Accessed: 05 January 2024).

16) Peng, C. (2022) CAC issues landmark rule to rein in Deepfake Misuse, Lexology. Available at: https://www.lexology.com/library/detail.aspx?g=a8dda00e-1f3b-4c99-a098-2a9e395d8c65 (Accessed: 05 January 2024).

17) Jayanta Deka / TNN / Updated: Sep 10, 2013 (no date) Muzaffarnagar riots: On Social Media, rumours and Anger: India News - Times of India, The Times of India. Available at: https://timesofindia.indiatimes.com/india/Muzaffarnagar-riots-On-social-media-rumours-and-anger/articleshow/22446959.cms (Accessed: 05 January 2024).

18) India Hunts 'Fake News' spreaders after anti-Muslim attacks (2021) The Guardian. Available at: https://www.theguardian.com/world/2021/nov/07/india-hunts-fake-news-spreaders-after-anti-muslim-attacks (Accessed: 05 January 2024).

19) Arun, C. and Nayak, N. (2016) Preliminary findings on online hate speech and the law in India, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2882238 (Accessed: 05 January 2024).

20) Samuels, E. (2020) How misinformation on WhatsApp led to a mob killing in India. Available at: https://www.washingtonpost.com/politics/2020/02/21/how-misinformation-whatsapp-led-deathly-mob-lynching-india/ (Accessed: 05 January 2024).

21) Arun, C. (2019) On WhatsApp, rumours, lynchings, and the Indian Government, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336127 (Accessed: 05 January 2024).

22) Standard, B. (2023) AI-powered deepfakes rise in 2023; concerns of its impact on privacy, Business Standard. Available at: https://www.business-standard.com/technology/tech-news/ai-powered-deepfakes-rise-in-2023-concerns-of-its-impact-on-privacy-123123100076_1.html (Accessed: 05 January 2024).

23) Aakash Sharma, Bollywood to war: How the year of deepfakes unfolded, India Today (Dec. 22, 2023), https://www.indiatoday.in/india/story/deepfake-artificial-intelligence-cyber-crime-elections-bollywood-actors-digital-world-2479431-2023-12-22.

24) 'Sextortionists' target celebs, Times of India (Feb. 23, 2021), https://timesofindia.indiatimes.com/city/mumbai/deepfake-clips-sextortionists-target-celebs/articleshow/81162493.cms.

25) Journalist Rana Ayyub Is Fighting to Expose the Truth in India, TIME (Oct. 22, 2021), https://time.com/6108251/rana-ayyub-india-journalism-modi/.

26) Kugler, M.B. and Pace, C., 2021. Deepfake privacy: Attitudes and regulation. Nw. UL Rev., 116, p.611.

27) Karen Hao, A horrifying new AI app swaps women into porn videos with a click, MIT Technology Review (Sept. 13, 2021), https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/.

28) Pawelec, M., Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions, 1 Digital Society 19 (2022).

29) Ziegler, Z., 2023. Michael polányi's fiduciary program against fake news and deepfake in the digital age. AI & SOCIETY, 38(5), pp.1949-1957.

30) Shruti Tomar, 4 FIRs lodged in Indore against deepfake videos of politicians on social media, Hindustan Times, (Nov. 27, 2023).

31) Nilufer Bhateja, Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India, SCC Blog (Mar. 17, 2023), https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/.

32) Nalini Sharma, Deepfake videos, images storming internet: What laws can come to your rescue?, India Today (Nov. 7, 2023), https://www.indiatoday.in/law/story/deepfake-videos-images-storming-internet-what-laws-can-come-to-your-rescue-2459655-2023-11-07.

33) Malkar, A.S., 2022. Right to Be Forgotten: Need for Constitutional Recognition in India?. Jus Corpus LJ, 3, p.615.

34) Singh, A.P. and Setia, R., 2018. Right to Be Forgotten-Recognition, Legislation and Acceptance in International and Domestic Domain. Nirma ULJ, 8, p.37.

35) Lucy Rana & Shilpi Sharan, Protection of Personality and Image Rights in India, 1 THE IP PRESS L.REV. (2022).

36) Sainath, S., 2022. The Right to Personality and Its Interplay with Intellectual Property Laws: An International Analysis of Character Merchandising. Issue 5 Int'l JL Mgmt. & Human., 5, p.978.

37) Vikrant Rana, Personality rights from Amitabh Bachchan to Sushant Singh to Anil Kapoor: Indian and Global View Point, (Nov. 3, 2023), https://www.barandbench.com/law-firms/view-point/personality-rights-amitabh-bachchan-sushant-singh-anil-kapoor-indian-and-global-view-point.

38) Fraga-Lamas, P. and Fernandez-Carames, T.M., 2020. Fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. IT professional, 22(2), pp.53-59.

39) Mahmud, F., Abdullah, Y., Islam, M. and Aziz, T., 2023. Unmasking Deepfake Faces from Videos Using An Explainable Cost-Sensitive Deep Learning Approach. arXiv preprint arXiv:2312.10740.

40) Leo Kelion, Deepfake detection tool unveiled by Microsoft, (Sept. 1, 2020), https://www.bbc.com/news/technology-53984114.

41) Jaclyn Diaz, Facebook Researchers Say They Can Detect Deepfakes And Where They Came From, (June 17, 2021), https://www.npr.org/2021/06/17/1007472092/facebook-researchers-say-they-can-detect-deepfakes-and-where-they-came-from.

42) IT Minister Vaishnaw, The Indian Express (Nov. 23, 2023), https://indianexpress.com/article/india/new-regulation-deepfakes-soon-vaishnaw-social-media-platforms-9039093/.