Open Access Library Journal
2025, Volume 12, e13311
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Cyber Crime or Technological Epidemic? Intersecting the Criminalization of *Sexual Deepfake* in Domestic and International Law

Evnat Bhuiyan[1*], Shariful Islam[2#], Abdullah Al-Mamun[3], Asraf Uddin[3]

[1]School of Social Sciences, Humanities and Languages (SSHL), Bangladesh Open University, Gazipur, Bangladesh
[2]Department of Law, Green University of Bangladesh, Dhaka, Bangladesh
[3]Department of Law, Leading University, Sylhet, Bangladesh
Email: *evnat.jnu.csgj@gmail.com, shariful@law.green.edu.bd, mamun@lus.ac.bd, asrafuddin709@gmail.com

How to cite this paper: Bhuiyan, E., Islam, S., Al-Mamun, A. and Uddin, A. (2025) Cyber Crime or Technological Epidemic? Intersecting the Criminalization of Sexual Deepfake in Domestic and International Law. *Open Access Library Journal*, **12**: e13311.
https://doi.org/10.4236/oalib.1113311

Received: March 20, 2025
Accepted: May 24, 2025
Published: May 27, 2025

Abstract

Researches on artificial intelligence (AI) usage primarily pivot to its positive utilization in different sectors while advanced AI tool like deepfake technology generating nudity and sexual photos or videos, however, got nominal academic attention. The study intends to address that vacuum examining the status of sexual deepfake in national and international legal spheres with a view to advocating the criminalization and penalization of sexual deepfake as a distinct offence. For portraying the importance of criminalizing sexual deepfake, the authors analyzed various examples of AI induced sexual violence, existing laws on deepfake, statutory actions for penalization, rationale behind criminalization, its challenges and solutions. A systematic literature review is done on deepfake, methods of deepfake detection and mitigation algorithms. The authors found no specific law on sexual deepfake either nationally or internationally. It is evident that existing cybersecurity, data protection or privacy laws are significantly insufficient to confront the boggling expansion of sexual deepfake. This lawlessness signifies the emerging threats and vulnerability of the victims of sexual deepfake. Formulating an International Covenant on the Protection from Artificial Intelligence Generated Violence would be one of the best safety gears to minimize the legislative vacuum in the global scenario as well as solving the statutory gaps of countries in determining the methods to control deepfake usage. Also, establishing deepfake detection and pornography detective website mechanism to check the sexual violence perpetuation might be a great help for initiating national level counter measures. Also, in addition to the regulatory mechanism, legal compliance, regulatory institutional estab-

*First author. Lecturer of Law.
#Corresponding author.

lishment and ethical standard, AI detection models using AI algorithm can be an effectually trustable way to ensure AI deepfake detectability. By introducing specified convention and statutory laws and adopting AI learning models as detection weapon, deepfake criminalization can be expediated. Moreover, the study aspires to promote further research in sexual deepfake criminalization that can enhance statutory and judicial activism, execution of laws, regulatory compliance to build a healthy safer cyberspace in digital earth.

Subject Areas

International Law, International Law of Cyberspace, International Criminal Law, International Human Rights Law

Keywords

Sexual Deepfake, Artificial Intelligence, Deepfake Pornography, Criminalization, Digital Integrity, Privacy and Dignity

1. The Genesis of Deepfake Technology

In the era of digitalization, deepfake technology is a new Artificial Intelligence (AI) weapon that generates sensory illusion and constant threat to individual freedom and dignity. Deepfake is raising modern doppelganger syndrome among youths causing consistent technological violence resulting in identity deception, severe violation of individual privacy rights, personal digital integrity, sexual defamation and cyber bullying. Deepfake is one of the buzzing AI specialized technologies recurrently used in making various virtual threats to defame individual identity by dispersion of adulterated information in the form of identity scam [1], national security threat [2], political statement manipulation [3] [4], financial blackmailing, deceitful media coverage [5], social turbulence [6] and national security menace [7].

Deepfake technology can create fake image and represent a person's image or voice as his own with fraudulent use of artificial intelligence. By this AI tool, image of face, part of body or even an entire body can be cut and added into another image or video flawlessly that looks completely real and undistinguishable. These activities can bring both blessings and disaster depending on the intention of the user.

Originated from 2017 after a *Reddit* platform user sponsored Celebrity Sexual Deepfake [8] many contends that previous deepfake platforms were associated with computer or technical expertise or tech-skill development but later other famous deepfake porn site like *MrDeepfake.com* (*MDF*) engaged in deepfake pornography circulation [9]. Goggle search traffic astoundingly increased in MDF after that, with a monthly 17 million visitors [10]. Sexual deepfakes are the most ferociously alarming usage of deepfake for committing sex crimes. More than 250 UK celebrities faced deepfake porn encounter [11].

A Deepfake website named *ClothOff.io* is an AI undressing website by *PornDude.com* that offers the service of undressing any woman's image at free of cost. 96% Deepfake elements are non-consensual porn or porn-associated sexual content, mostly women-oriented and targeted [12]. Sexual deepfake content generation and imagery fraud rocketed to 400% in 2022-2023. An independent researcher found 250,000 sexually explicit deepfakes on 35 of the most popular deepfake pornographic websites in last seven years with 3,50,000 nude photos in further 300 porn websites [13].

In 2023 alone 143,733 deepfake porn videos were uploaded to the 40 frequently visited deepfake pornography websites [14]. Be it Taylor Swift or Rashmika Mandana's image manipulation resulting in privacy disaster or Elon Musk's Cryptocurrency fake plan rumor causing him striking financial loss, the demerits of shifting Deepfake accessibility from professional experts to common public are clearly visible now [15].

2. Literature Review

Research conducted over 16,000 survey participant behavioral response of 10 countries expounded that deepfake pornography is a treacherous disorder that drastically destroy human mental faculty and even specified legislation on Non-consensual Synthetic Intimate Imagery (NSII) is proven to be unsuccessful to stop it [16]. The most valiant reason why sexual deepfake will be used more maliciously than intellectually is that it can extract real image and voice that can instigate sexual fantasy causing uncontrolled desire of sex enabling an outrage of digitally sexual misconduct [17], female objectification [18], exacerbating image based sexual violence (IBSV), deepfake pornography for blackmailing with fake porn [19], normalization of pornographic content [20], child sexual abuse materials (CSAM) through Deep Web [21], Online streaming of child sexual violence and misuse [22] as well as revenge porn [23]. Researchers experimented 12 risks including surveillance, cyber threat, misrepresentation, physiognomy, and objectionable exposé [24]. Detection methods are mostly proven to be difficultly faulty in deepfake identification [25]. However, some researchers suggest that deepfake cause no trust issue [26]. Also, researchers have shown detection techniques through user perception analysis on how automated and manually deepfake can be detected but sadly found the tactics to be erroneous and unsuccessful too because users utilize their mental faculty which is biased in most of the time [27]. Academic researches purely on sexual deepfakes are noticeably insufficient, most deepfake studies conducted are conceptual and danger-associate [28]. In addition, studies specifically focused on legal aspects especially on promulgating an international legal code to preach digital wellbeing, creating awareness, directing its contracting parties to penalize sexual deepfake via national statutory legislation are significantly inadequate. Thus, this research aims to address this research gap portraying the necessity of promulgating a universal convention and domestic legislations on sexual deepfake in international and national legal arena for protecting the right to pri-

vacy, right to cybersecurity, right to digital integrity, right to dignity ensuring cyber protection.

3. Objectives of the Study

The primal motto of this study is to venture the dark side of deepfake technology and to scientifically explore the fact whether sexual deepfakes are offence under international or national laws and principles. The study attempts to assess the rampant use of AI deepfake in committing crimes in cyberspace and digital platforms by spreading the electronic version of violence in order to defame an individual. In addition, the study recommends some possible ways to prevent the deepfake violations.

4. Research Question

A) Are sexual deepfake contents specifically criminalized as a statutory offence by any State?

B) What is the current regulatory status for sexual deepfake internationally?

5. Methodology of the Study

The paper is normative doctrinal research with statute-based, explorative, discussive and regressive analysis. The authors explored Google Scholar, MDPI, and PubMed for existing analyses on the artificial intelligence with the keywords—*Deepfake*, *Deepfake as AI violence*, *Legal status of deepfake*, *Deepfake criminalization*, *Deepfake pornography*, *Deepfake sexual terrorism*. At first, we have dived into the reasoning of criminalization with a short thematic brief on deepfake functioning and the devastating impact when it becomes sexually motivated containing non-consensual sexual imagery. We have presented an analysis of the existing laws exclusively on deepfake, laws that included deepfake as prohibited act or made punishable and how no single laws are there to treat sexual deepfake as a separate offence. Lastly, we have discussed the challenges of criminalization and provided recommendation on how deepfake criminalization can be formulated technically and technologically. Among the total 140 documents downloaded, 80 published documents i.e., journal articles, books, international reports, conference proceedings, working papers, statistical reports, thesis, newspaper articles etc. were read, analyzed, cross checked in consistent with the research objectives and utilized simultaneously. The authors used the term deepfake to indicate both image, video and audio deepfakes including image based animated videos produced from deepfake technology.

6. Identity Deception and Technological Pretension: How Deepfake Is Functioned

Deepfake is an artificially intelligent algorithm capable to procreate forged form of both audio or video content by combination of several neuronal grid methods inside smart automatized machine learning artificial intelligence. Autoencoder or

the Generative Adversarial Networks (GAN) are making the faking system's unidentifiability, unrecognizability by human intelligence very intact and solid in one hand while creating realistic portrayal of fake element on the other hand [29]. There used two neural networks *actor* and *critic.* The *actor* imitates the actual video or audio's motions and expressions and the *critic* distinguishes true from fraudulent content and both networks compete to confuse *critics* until they can't tell real from fake videos [30] [31].

Deepfake can believably picturize fake footage, fake voice, fake scheme, fake announcement which never occurred, told, done in real [32]. Machine learning and deep learning combinational data distribution has created several deepfake AI tools that will change the reality of human existence into an unrealistic non-existential reality in futuristic view by publicizing information in the form of image, audio and video which will not be possible to trace, stop, detect or control due to constant technological development, functional upsurge, fluctuating algorithms and intensification in new models of data distribution generative models [33]. Deepfake is a combination of different AI algorithms, Generative Adversarial Networks (GANs) and Convolutional Neural Networks (CNNs) that produces Artificially Synthesized Media (ASM) having damaging and degrading contents [34]. Sexual deepfakes are just focused on online contents works to depreciate woman dignity.

7. Forms of Sexual Deepfakes

Deepfake arouses gender based sexual violence [35] as a digitalized version being an added volume to the existing gender-based violence (GBV) [36]. Sexual deepfakes are fiercely utilized as a method to degrade woman mostly in order to extort financial gain from various online platforms or directly from the targeted victims by blackmailing. Apart from image based sexual blackmailing [37], there are other forms of sexual deepfakes causing serious concern for women safety.

7.1. Cybercrime and Sextortion

Being an advanced computational intelligence, deepfake has ability to reason, response, detect and has problem-solving skill like humans which makes it able to commit cybercrimes indiscriminately [38]. Therefore, sextortion has become a predominant source of financial blackmailing to male persons [39] because deepfake contents can acutely be used to sextort.

7.2. Deepfake Pornography

This is inflicted particularly targeting women resulting in sexual privacy violation, close partner exploitation [40], acute attack upon personal dignity and reputation, and unbearable psychological stress [41].

7.3. Deep Nude: Deep Disease with No Antidote?

Deep Nude app can make a clothed body naked and a naked as clothed with effortlessly skilled way that resembles to real picture of the person in the photo.

Although developer of Deep Nude withdraws the app as soon as it creates bizarre controversial depiction of images, dejectedly, an already circulated app in the internet world cannot be deleted permanently.

8. Criminalizing Deepfake

Criminalization of deepfake technology is highly dubious due to different cultural and legal setting across countries. A fundamental problem is that creation of deepfake is not an offence; rather sharing deepfake is made punishable [42]. Here lies the ultimate uncertainty for the Deepfake criminalization. Deepfake is basically face forgery [43] website that targets *Face* for its content. This makes the technology the scariest because face reveals the vital organ of human body and an inconvincibly strongest identity of human. Indiscriminate usage of face exchange application like *Face2face*, *Face swap*, *Magic Swap Puzzle*, *my Fake App and Deep Face Lab* is accelerating rapidly among youth as a podium of fun adventure and entertainment. But the status of face as an inevitably fundamental part of a human natural person's body and physical appearance is requestioned by scholars as to whether biological face replaced by digital face can be an issue of legal violation in the sense that digital face is different from human face [44].

Deepfake is successfully used in cinematic development VFX [45], news anchorage substitution, gaming text to speech AI technology alternative to voice over artist and budget saving for advertising commercials, photographic inventiveness, in open distant learning as an educational tool, video conferencing or research endeavors [46]. Entertainment industry has witnessed enormous success in propelling unparallel visualization creativity and uniqueness in producing entertaining artistic expression in the art and film business [47]. Deepfake therapeutic treatment to psychological moral injury patients has been beneficial [48].

But the misuse of deepfake is alarmingly shocking [49] committing serious criminal acts punishable under law [50]. Sexual deepfake causes acute cyber humiliation by propagating hateful comments on social media platforms, extreme privacy threat, wrongful media depiction, blackmailing, sextortion, slanderous libel [51], social media disinformation spread [52] and other acts that destroy a person's dignity and freedom. These are vehement violation of constitutional and legal right to privacy, digital wellbeing and integrity, online safety, dignity, liberty. Also, it causes unnecessary sexual harassment and further criminal activities of financial embezzlement or fraud. Hence, the criminalization of Sexual deepfake is unhesitatingly mandatory.

Differences in jurisprudential understanding of legal personhood that liability can only be borne by a natural human or legal enterprise and fundamental criminal element of *mens rea* i.e., guilty intention, is absent in AI because AI tools cannot be conclusively functioned to have natural psychological emotion [53]. But if any act or omission required is not done or done anything prohibited by law or any negligence using AI technology, the AI user can be held criminally responsible which can ensure the deepfake criminal liability [54].

9. Evidences on Inadequacy and Inefficiency of Deepfake Legislation

As there is no uniform overtly consistent international legal mechanism for deepfake, more importantly, sexual deepfake, thus, countries started to promulgate regulatory framework and penal laws to address the deepfake AI abuse. The European Union Artificial Intelligence Act 2024 (EU AI Act) is so far the only international instrument addressing artificial intelligence misappropriation. It defines Deepfake in its Article 3(60) as synthetic virtual data pretending to be authentic. Regrettably, the Act fails to integrate the sexual abuse borne from deepfake. Nevertheless, EU Digital Services Act (DSA) imposes fines to the websites and online directories containing deepfake or other offensive or negative AI produced contents for non-removal in due process and time [55].

For national legislation, the United States, the United Kingdom, China and South Korea have so far promulgated specific legislation for deepfake but no laws for particularly prohibiting sexual deepfake. United States federal legislation of National Defense Authorization Act (NDAA) with six US provincial states banning deepfake misuse and three states particularly prohibiting nonconsensual deepfake pornography with fines of up to 2,500 USD or rigorous prison of up to 12 months under Article 230 of the Communications Decency Act of 1996, China's Deep Synthesis Code of stringent restriction on deepfake content, United Kingdom's Online Safety Act 2023 punishing sharing deepfake porn and Criminal Justice Bill 2024 are some of the current legislative attempts to curb deepfake spread and label wrongful use of deepfake [56]. However, deepfake pornography or other sexual deepfake just got nominal attention or legal redress and remains unaddressed in larger extent. Whereas adult pornography control is itself a biggest challenge for law enforcement, deepfake pornography is even more difficult to trace. Basically, it is untraceable as to which adult contents are non-consensual because it is not possible to distinguish whether the content is originally obtained user consent, commercially exploited or produced as a part of revenge porn which has no business involvement.

The European Union (EU) passed robust data protection statute called General Data Protection Regulation (GDPR) that categorizes deepfake as privacy, anti-harassment or cyber threat but not as a distinct offence considering it as a similar offence like pornography [57]. The EU Acts did not primarily aim deepfake criminalization rather presented stringent policies on privacy violation and also pointed at the matter of unauthorized individual data usage [58]. Thus, scholars are of the view that if deepfake and revenge porn is classified under pornography Act rather deepfake legislation, it will be useless [57].

The Indonesia's legislative approaches such Electronic Information and Transactions (ITE) Law and other Personal Data Protection Law have failed to regulate deepfake offences for which scholars have demanded legislating statutes on specified deepfake detection, AI ethics and global effort to minimize the rapid ever-increasing blowout of deepfake [59].

US has so far been the only federal country with explicit address to deepfake porn by introducing federal laws like Malicious Deepfake Prohibition Act 2018, Deepfake Accountability Act 2019 and Deepfake Report Act 2019 [6] and new bills No Fakes Act, No AI Fraud Act etc., [60]. The Korea Communications Standards Commission (KOCSC) blocked many deepfake websites in 2023 making nonconsensual sexual deepfake content punishable with five years in prison with a $250,000,000 fine and commercial distribution with seven years in prison [61]. Nonetheless, these statutes are focused on deepfake pornography which is only one category of sexual deepfake. Thus, a comprehensively inclusive punitive statute covering all genres of sexual deepfake including privacy, dignity, personal integrity, cyber safety and data protection is not formulated in any country till today.

10. Legislative Challenges of Imposing Legal Proscription on Deepfake

a) International: Challenges of making international convention on deepfake prohibition is concerned with the legality and non-consensual issues. The first hurdle is however to define deepfake due to its unpredictability. Universal definition for deepfake is a tough chase as AI models can reach up to unimaginable extent, nature, genre, forms like audio or video and classification which even can be unknown to AI creators. Forming international consensus might be difficult due to its unconventional nature and cultural aspect.

Promulgating a separate convention might be a good start, but nations might not incorporate with the obligation to make specific national Acts on deepfake. Next, is the issue of pornography which is itself an extremely unregulated offence throughout the world due to the disputed and different approaches of States towards it, some States legalizing porn while others condemning it is another misnomer equally applicable for deepfake pornography as well. Cyber laws are yet another cause of challenge for creating deepfake convention because cyber security mechanism is not fully established yet as a reliable sector to chase online harassment across the world.

b) National: Challenges of implementing domestic legal restrictions are mostly related to affordability and execution. The most glaring challenge for national legislation for criminalizing deepfake is to fix the regulatory mechanism and provisions on deepfake detection. Deepfake is functioned by high end AI algorithms which needs separate process to be detected and regulated. For punishing deepfake creators, first strong regulatory mechanism is to be set up but many nations either cannot afford to those technology that can trace deepfake or simply overlook due to pornographic legality in their nations. States legalizing adult content or allows adult industry to run legally will find it extremely difficult to identify non-consensual deepfake pornography. Moreover, statutes particularly framed for online safety of woman are rare, even if there is any statute for tackling online harassment to women, it does not specify the sexual deepfake as a category of online harassment. Furthermore, sexual deepfake is not even categorized as a

mainstream offence and is not included as an offence under specific provision of any penal law. These challenges put the criminalization of sexual deepfake under utmost uncertainty risking millions of individuals privacy, dignity and integrity into massive threats of blackmailing.

11. Sexual Deepfake Control: Scope for Resorting to Criminalization

11.1. How AI Itself Is a Solution to Deepfake Detection

For deepfake detection and criminalization, a rigorous collaborative effort from tech experts and media giants is needed for. It is fundamental to develop AI detection mechanism before promulgating statutes criminalizing deepfake because government must address how to identify deepfake. Without this, mere legal criminalization will not bring any fruits. Very few countries are actively working to control deepfake by setting laws and regulations inflicting higher penalties.
But rarely any State is working on deepfake circulation, publication and detection mechanism—which are the foremost ways to stop deepfake maniacs. Deepfake manipulation can be tackled by the very AI based Deepfake Detection System (DDS) [62]. Deepfake controlling AI methods like Convolutional Neural Network (CNN) or Long Short-Term Memory (LSTM) methods by extracting features of the frame image of a video using a CNN, Eye blinking by LSTM etc. are some of the earlier methods that were proposed as deepfake detection method [63]. Nonetheless, a more reliable process of extracting layers of any modifications of frames or the computer vision features of the digital content is proven to be more accurate having 96% - 97% detection rate [64].

Scholars suggested blockchain method to detect deepfake content from internet service providers [65] [66]. Another way to detect fake and fabricated deepfake videos/images is the use of Ethereum smart contracts which identifies the history of the content to its original source by tracking [67]. Blockchain-based federated learning (BFL) and data normalization techniques are considered as effective in tracing deep learning technology [68]. Interestingly, deepfake can not only be traced but also be removed using AI technology. XAI-ART i.e., Explainable AI (XAI) coupled with Adversarial Robustness Training (ART) is such AI technique to combat deepfake ensuring its removal [69].

By applying machine learning models and tracking alterations anomaly in larger dataset deepfake can be identified and controlled. Combining various AI detection models is possibly the best strategy to cope with deepfake enigma [70]. Also, building technological surveillance on AI by establishing AI generation regulatory authority can be topnotch thought [71]. OpenAI implemented DALL-E to detect deepfake image with proven 98% accuracy but with limitation that no video content can be traced and only AI made by them can be checked by this software application [72].

By regulating the incorporation of these AI technologies and the inventors to instill moral methodical approach into the functionary part of these AI tools like

deepfake can be a method to curb sexual deepfake [73]. One proven example is the Thai AI Chatbot *LAW-U* developed by Natural Language Processing (NLP) combining 182 Thai Supreme Court verdicts for suggesting sexual deepfake victims or survivors' legal knowledge by referring appropriate judgements on sexual violence. It gained 88% success making it capable for execution in addressing real deepfake problems [74].

Sexual deepfake will be redressable by reinforcement of privacy, personal integrity, dignity centric victim protection rights by executing penal law mechanism so that any violation to a person's dignity can strictly be handled under statutory punishment. AI deepfake is an extremely complex computer algorithmic data sets that are beyond perceptibility or captivation, even beyond the very human imagination who have invented [75]. Therefore, for the AI deepfake perpetuating sexual violence as an invisible identity miscreant, it is the very AI algorithm which knows the way out how to mitigate the wrongful usage of deepfake and what data sets will be useful to create user limitation or restricted accessibility [76].

11.2. Legislative Measures for Deepfake

After ensuring the technological support system and nationally backed up arrangements such as deepfake prevention unit with cyber units, States must criminalize deepfake by promulgating an Act particularly for sexual deepfake with stringent punishment. The Act will define the nature of legal and illegal deepfake. It will categorize the features of wrongful deepfakes and how an online content will be considered illegal deepfake. It will mention different method and acts of generating sexual deepfake and can compose a board to regulate a domestically controlled deepfake detection system and implement the law. The Act will have severe punishment according to the types of destruction the victim faced and can enlist this as both criminal and civil law violation.

Like in most pornography statutes, pornographic contents are banned from being produced, marketized, stored, distributed, circulated, commercially used, uploaded in any online platform without consent or wrongfully for blackmailing, sexual deepfake can be framed up in similar way while making deepfake prohibition laws.

11.3. Other Measures for Deepfake Prevention

AI technology monitoring system and psychological motivation for creating resistance in the user mind for not committing crime [77], strong regulatory body to limit and control deepfake technology and apps [56], blocking deepfake porn websites, separate law for deepfake and tortious remedies for sexual privacy protection and corporate social governance [78], media literacy [79], AI detectability by forensic experts for judicial trial [80], ensuring ethical healthy AI and deepfake use [81] are some of the measures that are suggestible for all countries to maximize deepfake detachment and minimize its misapplication. Europe has adopted a unique right named "Right to be forgotten" (RTBF) which resembles the concept

that any indecent information in the form of image, video or audio should be forgotten gradually as soon as it got released in the society [61]. The RTBF approach was introduced as a social simulation policy to protect deepfake victims' moral right to be respected, to protect the victims from public bashing so that they do not have to suffer from fame-shaming, name-shaming or body-shaming. AI ethics is, therefore, tremendously imperative for controlling deepfake technology.

12. Findings

It is found that sexual deepfake is not considered as a separate offence, rather, few laws consider it as a category of cybercrime or tech crime. There exists a latent scarcity of national and international legal mechanism specifically designed to monitor or mitigate sexual deepfake. Neither specific national regulatory laws, nor any provisions on unauthorized or malicious use of deepfake is found. Intentional deepfake usage has been banned in handful of countries or made punishable with stricter penalty but in very few ones with immense limitation.

Banning by statutes will not come in rescue in case of sexual deepfake. These laws are insufficient to cop up with variety of AI violation of different fields, are not exclusive to sexual deepfakes and deepfake pornographic content, have no specific regulatory process for privacy and sexual integrity violation via deepfake. The remedy process is celebrity focused and not public oriented. Overall, the sexual privacy protection is greatly missing in existing limited legislations. For that firstly we need an International Convention on sexual deepfake for setting international attention and penalty rules for combating AI criminal usage challenges. Countries must resort to tech-enhanced solutions before implying criminalization of sexual deepfakes. It is because prosecuting criminal cases on sexual deepfake will have the requirement of solid evidence whether the content of debate committed any crime using deepfake technology. For that, the victim needs to resort to the technology which will prove the deepfake authentication for trial procedure.

Basically, it goes on both ways by criminalizing deepfake, government will have to incorporate measures to implement deepfake detection. For that, existing legislations needs to be revised in greater level to enhance privacy protection of victim of sexual deepfake crimes. Thus, the triangular effect needs to be understood—laws on AI and deepfake needs to be promulgated and existing laws must be strengthened. This will lead to better execution of judicial decision on victim of crimes of sexual deepfake.

For formulating laws, the AI detection mechanisms must be established that can work in full swing. Henceforth, it is pertinent to criminalize the deepfake utilization on sexually motivated or targeted activities conducted to defame the dignity, integrity and privacy of the endless victims across the world. Strong combination of law and enforcement, judicial remedy and technological advancement can stop this. For all these sectors to work out, we need an international measure that can compel its contracting parties and create indirect pressure on States to adopt laws on criminalization of sexual deepfake by differentiating the usage of deepfake in

sexual and non-sexual purposes. The core problem is differentiating sexual deepfake from deepfake is not possible because not all deepfake contents are negative, negatives are not always sexualized and the deepfake are circulated, generated and publicized in gargantuan size through many authorized and unauthorized websites and online platforms or social media applications. Thus, detecting, blocking, penalizing are the steps to stop sexual deepfakes. For this, we need to criminalize sexual deepfakes not as an ancillary to pornography or revenge porn or privacy invasion but as a specific offence having specific identification and penalty.

13. Recommendations

Sexual deepfake should be recognized as a distinct offence and it should be regulated via national and international initiative. Deepfakes need to be addressed academically and legislatively and judicially. The paper simply proposes a dual-mode activism of strategic remedy as an all-out probable plan for expected controlling of sexual deepfakes in order to facilitate the entire criminalization process—a) Technological remedy b) Legislative and legal remedy. Firstly, for the technological solution, the following approaches need to be established, enhanced, reintroduced and strengthened:

i) Generating and developing strong Deepfake Detection System (DDS) by national level top technological companies including cyber units using methods like machine learning, watermarking, blockchain technology,

ii) Establishing deepfake pornography detective AI website mechanism,

iii) Anti-deepfake technology for sexual deepfake,

iv) Advanced AI laboratory for tracing sexual AI picture rotation,

v) Developing software and algorithms to monitor the source, size, specificity of sexual content,

vi) Capacity building by technological knowledge dissemination is to be done.

For the legal remedy, we are on the view of following the below mentioned tactics and steps of legal approaches to properly execute the technological remedy:

i) Universal criminalization of malicious use of deepfake,

ii) Convention on Protection from Sexual Deepfake or Universal Sexual Deepfake Protection Covenant,

iii) Separate enactment for sexual deepfake such as nonconsensual deepfake adult pornography, deepfake child pornography, nonconsensual counterfeit sexual image-audio-video based depiction and child abuse,

iv) Specified artificial intelligence and deepfake provisions in the existing laws on pornography,

v) Emphasizing tort laws for defamation and violation of personal reputation;

vi) National digital policy on sexual deepfake,

vii) Strengthening prevention of sexual e-crimes and cybercrimes,

viii) Robust information and communication technology, data protection, data privacy, data integrity and cybersecurity,

ix) Operative social media regulation by establishing AI Deepfake Misuse Mon-

itoring Authority for holding deepfake porn streamers or distributors, website owners and deepfake criminals under laws with stringent penalty for deepfake circulation and non-removal of deepfake content after proven misconduct; and

x) Distinct defamation statute for IBSV deepfakes. High tech AI laboratory and AI expert professional developers to crosscheck AI deepfake authenticity for punishing criminals in judicial proceedings.

Government can implement these recommendations by setting liaison with different collaborators of ministries, policy makers, tech organizations, software companies, online content distributors, media specialists, researchers and internet service providers. For international convention, big States need to think about deepfake on serious note with real intention to prevent deepfake, particularly sexual deepfake. The legal system has to evolve with the technological development to control the far-reaching adverse impact of sexual deepfake. For this, government must head to policy making on deepfake detection, control, prevention mechanisms and set up legal remedies by criminalizing deepfake. National policy adoption on cybersecurity, privacy of child and woman including control of data manipulation are some of the aspects State has to actively take initiative to make policies. For implementing policies, legislators must promulgate a law on sexual deepfake control and prevention, identifying nonconsensual content, blocking deepfake porn sites, controlling internet service providers, making surveillance rooms of cyber units for online platform or setting deepfake detection units as a part of different cell of cyber security force. All these efforts will bring out successful control of sexual deepfake if deepfake is criminalized with clearly statutory provision and legally recognized as offence.

14. Conclusions

Sexual deepfake is a severe peril for public security, a serious threat to society. In the name of entertainment or social media influence, this AI tool is creating unimaginable hazard for woman and girls in particular, which if not regulated by law will cause an imagery epidemic for the right to dignity and freedom for the female section of society.

Unfortunately, the illegality of deepfake is still debatable and no concrete laws have been pronounced in criminalizing malicious usage of artificial intelligence let alone deepfake as a statutory offence or as a violation of international laws. Once we stepped into the artificiality as a replacement of human intelligence and capacity to solve complex problems, it has already become an integral part of human life and will shape its future. The paper emphasizes the criminalization and sufficient legal framework to suppress the application of sexual deepfake.

But criminalization, laws, regulatory bodies or whatsoever, is not the only cure to sexual deepfake. Is promulgating an inclusive Deepfake Offence (Prevention, Punishment and Protection) Act on country level will be a feasible solution? May be, yes. But artificial intelligence requires more of a technological control than legal control. Regulatory action cannot enhance a zero virtual harassment society

and perhaps the ever increasingly tech-change will never bring back the real world to the viewers of upcoming generation. Cumulative efforts from government, computer scientists, tech researchers, AI specialists, intergovernmental organizations, civic society, awareness activists and advocacy groups should come forward with a determination and scientifically implementable plan to stop the sexual imagery, animated or motion violence like deepfake with the help of law enforcement organs.

Declaration

The authors confirm that the present manuscript or its content has not been published previously and not under consideration for publication in any other journal during the submission to OALibJ.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Dunn, S. (2020) Identity Manipulation: Responding to Advances in Artificial Intelligence and Robotics. Dalhousie University Schulich School of Law, Discussion Paper. https://doi.org/10.2139/ssrn.3772057

[2] Taylor, B.C. (2020) Defending the State from Digital Deceit: The Reflexive Securitization of Deepfake. *Critical Studies in Media Communication*, **38**, 1-17. https://doi.org/10.1080/15295036.2020.1833058

[3] Painter, R.W. (2023) Deepfake 2024: Will Citizens United and Artificial Intelligence Together Destroy Representative Democracy? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4558216

[4] Walker, C.P., Schiff, D.S. and Schiff, K.J. (2024) Merging AI Incidents Research with Political Misinformation Research: Introducing the Political Deepfakes Incidents Database. *Proceedings of the AAAI Conference on Artificial Intelligence*, **38**, 23053-23058. https://doi.org/10.1609/aaai.v38i21.30349

[5] Vaccari, C. and Chadwick, A. (2020) Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media+Society*, **6**, 1-13. https://doi.org/10.1177/2056305120903408

[6] Liu, M. and Zhang, X. (2023) Deepfake Technology and Current Legal Status of It. *Proceedings of the* 2022 3*rd International Conference on Artificial Intelligence and Education* (*IC-ICAIE* 2022), Chengdu, 24-26 June 2022, 1308-1314. https://doi.org/10.2991/978-94-6463-040-4_194

[7] Pawelec, M. (2022) Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. *Digital Society*, **1**, Article No. 19. https://doi.org/10.1007/s44206-022-00010-6

[8] Cole, S. (2022) How Sex Changed the Internet and the Internet Changed Sex: An Unexpected History. Workman Publishing Co.

[9] Timmerman, B., Mehta, P., Deb, P., Gallagher, K., Dolan-Gavitt, B., Garg, S., *et al.* (2023) Studying the Online Deepfake Community. *Journal of Online Trust and Safety*, **2**. https://doi.org/10.54501/jots.v2i1.126

[10] Gigazine (2023) Targeting Not Only Celebrities But Also Ordinary People, Where

AI-Made Deep Fake Porn Videos Are Bought and Sold on Sites That Hit Google Searches.

[11] Hannah Roberts, P.E.R. (2024) More than 250 UK Celebrities Are Victims of Deepfake Pornography, Probe Finds. Yahoo News. https://uk.news.yahoo.com/more-250-uk-celebrities-victims-205024051.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMxZW4UhZLRW4Jla52fwbIDriCamXhaGPaZETLdM-7nmeRERu3y9uLgMxlchjnxvn1VzZYXCQQpUjNu3cnVm42onH3tt1TbUd_CTr

[12] Sensity (2021) How to Detect a Deepfake Online: Image Forensics and Analysis of Deepfake Videos. https://sensity.ai/blog/how-to-detect-a-deepfake/

[13] Burgess, M. (2023) Deepfake Porn Is Out of Control. Wired. https://www.wired.com/story/deepfake-porn-is-out-of-control/

[14] Panda Security (2024) Deepfake Pornography Explosion. Panda Mediacenter.

[15] Arrigoni, L. (2024) Deepfakes and AI' New Threat to Security: The High Cost of Free Open-Source Generative Software. Cyber Defense Magazine. https://www.cyberdefensemagazine.com/deepfakes-and-ais-new-threat-to-security/

[16] Umbach, R., Henry, N., Beard, G.F. and Berryessa, C.M. (2024) Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries. *Proceedings of the* 2024 *CHI Conference on Human Factors in Computing Systems*, Honolulu, 11-16 May 2024, 1-20. https://doi.org/10.1145/3613904.3642382

[17] Kaushal, T. (2023) Women, Deepfake Pornography, and the Imperative of Legal Education in the Age of AI. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4597863

[18] Jacobsen, B.N. and Simpson, J. (2023) The Tensions of Deepfakes. *Information, Communication & Society*, **27**, 1095-1109. https://doi.org/10.1080/1369118x.2023.2234980

[19] Dunn, S. (2024) Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI. *McGill Law Journal*, **69**, 1-15.

[20] Mukta, M.S.H., Ahmad, J., Raiaan, M.A.K., Islam, S., Azam, S., Ali, M.E., *et al*. (2023) An Investigation of the Effectiveness of Deepfake Models and Tools. *Journal of Sensor and Actuator Networks*, **12**, Article 61. https://doi.org/10.3390/jsan12040061

[21] Ngo, V.M., Gajula, R., Thorpe, C. and Mckeever, S. (2024) Discovering Child Sexual Abuse Material Creators' Behaviors and Preferences on the Dark Web. *Child Abuse & Neglect*, **147**, Article 106558. https://doi.org/10.1016/j.chiabu.2023.106558

[22] Drejer, C., Riegler, M.A., Halvorsen, P., Johnson, M.S. and Baugerud, G.A. (2023) Livestreaming Technology and Online Child Sexual Exploitation and Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, **25**, 260-274. https://doi.org/10.1177/15248380221147564

[23] Santana, M. S. (2022) Justice for Women: Deep Fakes and Revenge Porn. 3rd Global Conference on Women Studies, 113-128. https://www.dpublication.com/wp-content/uploads/2022/02/27-10177.pdf

[24] Lee, H., Yang, Y., Von Davier, T.S., Forlizzi, J. and Das, S. (2024) Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks. *Proceedings of the* 2024 *CHI Conference on Human Factors in Computing Systems*, Honolulu, 11-16 May 2024, 1-19. https://doi.org/10.1145/3613904.3642116

[25] Leibowicz, C.R., McGregor, S. and Ovadya, A. (2021) The Deepfake Detection Dilemma: A Multistakeholder Exploration of Adversarial Dynamics in Synthetic Media. *Proceedings of the* 2021 *AAAI/ACM Conference on AI, Ethics, and Society*, Virtual,

19-21 May 2021, 736-744. https://doi.org/10.1145/3461702.3462584

[26] Etienne, H. (2021) The Future of Online Trust (and Why Deepfake Is Advancing It). *AI and Ethics*, **1**, 553-562. https://doi.org/10.1007/s43681-021-00072-1

[27] Mink, J., Wei, M., Munyendo, C.W., Hugenberg, K., Kohno, T., Redmiles, E.M., *et al*. (2024) It's Trying Too Hard to Look Real: Deepfake Moderation Mistakes and Identity-Based Bias. *Proceedings of the* 2024 *CHI Conference on Human Factors in Computing Systems*, Honolulu, 11-16 May 2024, 1-20. https://doi.org/10.1145/3613904.3641999

[28] Godulla, A., Hoffmann, C.P. and Seibert, D. (2021) Dealing with Deepfakes—An Interdisciplinary Examination of the State of Research and Implications for Communication Studies. *Studies in Communication and Media*, **10**, 72-96. https://doi.org/10.5771/2192-4007-2021-1-72

[29] Byman, D.L., Gao, C., Meserole, C. and Subrahmanian, V.S. (2023) Deepfakes and International Conflict. Foreign Policy at Brookings Institute.

[30] Yan, Y. (2023) Deep Dive into Deepfakes-Safeguarding Our Digital Identity. *Brooklyn Journal of International Law*, **48**, Article 8.

[31] Marin, A., Suriel-Luna, C. and Rai, S. (2022) The Effects of Deepfakes and How We Can Mitigate Them. https://openlab.citytech.cuny.edu/deepfakeproject/files/2022/05/Collaboration-project-final-draft-1.pdf

[32] Langguth, J., Pogorelov, K., Brenner, S., Filkuková, P. and Schroeder, D.T. (2021) Don't Trust Your Eyes: Image Manipulation in the Age of Deepfakes. *Frontiers in Communication*, **6**, Article 632317. https://doi.org/10.3389/fcomm.2021.632317

[33] Jacobsen, B.N. (2024) Deepfakes and the Promise of Algorithmic Detectability. *European Journal of Cultural Studies*, **28**, 419-435. https://doi.org/10.1177/13675494241240028

[34] Gilbert, C. and Gilbert, M.A. (2024) The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation. *International Research Journal of Advanced Engineering and Science*, **9**, 170-181.

[35] Laffier, J. and Rehman, A. (2023) Deepfakes and Harm to Women. *Journal of Digital Life and Learning*, **3**, 1-21. https://doi.org/10.51357/jdll.v3i1.218

[36] Hall, M., Pester, A. and Atanasov, A. (2022) AI Threats to Women's Rights. *Journal of Law and Emerging Technologies*, **2**, 88-51. https://doi.org/10.54873/jolets.v2i2.86

[37] Qiwei, L., McDonald, A., Haimson, O.L., Schoenebeck, S. and Gilbert, E. (2024) The Sociotechnical Stack: Opportunities for Social Computing Research in Non-Consensual Intimate Media. *Proceedings of the ACM on Human-Computer Interaction*, **8**, 1-21. https://doi.org/10.1145/3686914

[38] Rasyid, M.F.F., SJ, M.A., Mamu, K.Z., Paminto, S.R., Hidaya, W.A. and Hamadi, A. (2024) Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime. *Jurnal Ilmiah Mizani: Wacana Hukum, Ekonomi Dan Keagamaan*, **11**, 49-63. https://doi.org/10.29300/mzn.v11i1.3318

[39] Notté, R.J. (2024) Exploring the Impact of Sextortion on Adult Males: A Narrative Approach. *Technology in Society*, **78**, Article 102617. https://doi.org/10.1016/j.techsoc.2024.102617

[40] Graber-Mitchell, N. (2021). Artificial Illusions: Deepfakes as Speech. *Intersect*, **14**.

[41] Qin, L., Hamilton, V., Wang, S., Aydinalp, Y., Scarlett, M. and Redmiles, E.M. (2024) "Did They Consent to That?": Safer Digital Intimacy via Proactive Protection against Image-Based Sexual Abuse. arXiv: 2403.04659. http://arxiv.org/abs/2403.04659

[42] Durham University (2024) Deepfake Porn: Why We Need to Make It a Crime to Create It, Not Just Share It. Resaerch and Business. https://www.durham.ac.uk/research/current/thought-leadership/2024/04/deepfake-porn-why-we-need-to-make-it-a-crime-to-create-it-not-just-share-it/

[43] Naitali, A., Ridouani, M., Salahdine, F. and Kaabouch, N. (2023) Deepfake Attacks: Generation, Detection, Datasets, Challenges, and Research Directions. *Computers*, **12**, Article 216. https://doi.org/10.3390/computers12100216

[44] Marino, G. and Leone, M. (2024) The Legal Semiotics of the Digital Face: An Introduction. *International Journal for the Semiotics of Law-Revue Internationale de Sémiotique juridique*, **37**, 721-727. https://doi.org/10.1007/s11196-024-10122-6

[45] Bode, L. (2021) Deepfaking Keanu: Youtube Deepfakes, Platform Visual Effects, and the Complexity of Reception. *Convergence: The International Journal of Research into New Media Technologies*, **27**, 919-934. https://doi.org/10.1177/13548565211030454

[46] Nenovski, B., Ilijevski, I. and Stanojoska, A. (2023) Strengthening Resilience against Deepfakes as Disinformation Threats. In: Adamczyk, A., Ilik, G., Tahirović, M. and Zajączkowski, K., Eds., *Poland's Experience in Combating Disinformation: Inspirations for the Western Balkans*, Oficyna Wydawnicza ASPRA-JR, 127-142.

[47] Olson, A. (2021) The Double-Side of Deepfakes: Obstacles and Assets in the Fight Against Child Pornography. *Georgia Law Review*, **56**, Article 8.

[48] van Minnen, A., Ter Heide, F.J.J., Koolstra, T., de Jongh, A., Karaoglu, S. and Gevers, T. (2022) Initial Development of Perpetrator Confrontation Using Deepfake Technology in Victims with Sexual Violence-Related PTSD and Moral Injury. *Frontiers in Psychiatry*, **13**, Article 882957. https://doi.org/10.3389/fpsyt.2022.882957

[49] Romero Moreno, F. (2024) Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content. *International Review of Law, Computers & Technology*, **38**, 297-326. https://doi.org/10.1080/13600869.2024.2324540

[50] Sohail, M., Hamid, A., Kashif, M., Saqib, M. and Naz, H. (2023) Deepfake: Life & Law in the Age of Illusions & Manipulations. *Journal of Positive School Psychology*, **7**, 225-230.

[51] Rizzica, A. (2021) Sexually Explicit Deepfakes: To What Extent Do Legal Responses Protect the Depicted Persons? Analysis of the Italian Scenario through Criminal Law, Data Protection Law and Right to Image. Master's Thesis, Tilburg Law School.

[52] Chang, C. (2023) Revisiting Disinformation Laws in the Age of Social Media. *Arizona Law Journal of Emerging Technologies*, **6**, Article 4. https://doi.org/10.2458/azlawjet.5765

[53] Eurike Hailtik, A.G. and Afifah, W. (2024) Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia. *Asian Journal of Social and Humanities*, **2**, 776-795. https://doi.org/10.59888/ajosh.v2i4.222

[54] Gresmelian, A., Hailitik, E., & Afifah, W. (2023) Regulating Artificial Intelligence as a Perpetrator of Deepfake Crimes in Indonesia. *Proceedings of the 5th International Conference on Universal Wellbeing ICUW* 2023 *University of Indonesia*, Jakarta, 14-16 October 2023, 26-43. https://asasijournal.com/index.php/icuw2023/article/view/21

[55] Nasiri, S. and Hashemzadeh, A. (2025) The Evolution of Disinformation from Fake News Propaganda to AI-Driven Narratives as Deepfake. *Journal of Cyberspace Studies*, **9**, 229-250.

[56] Ramluckan, T. (2024) Deepfakes: The Legal Implications. *International Conference*

on Cyber Warfare and Security, **19**, 282-288.
https://doi.org/10.34190/iccws.19.1.2099

[57] Fernandez, A. (2021) "Deep Fakes": Disentangling Terms in the Proposed EU Artificial Intelligence Act. *UFITA*, **85**, 392-433.
https://doi.org/10.5771/2568-9185-2021-2-392

[58] Nair, A. (2018) The Regulation of Internet Pornography: Issues and Challenges. Routledge. https://doi.org/10.4324/9781315726892

[59] Judijanto, L., Utama, A.S. and Setiyawan, H. (2025) Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deep-Fake) in Indonesia. *The Esta Journal Law and Human Rights*, **3**, 101-109.
https://doi.org/10.58812/eslhr.v3i02

[60] Miotti, A. and Wasil, A. (2024) Combatting Deepfakes: Policies to Address National Security Threats and Rights Violations. arXiv:2402.09581.
http://arxiv.org/abs/2402.09581

[61] Monique, C., T., Wulandari, S. and Bhirini Slamet, A. (2024) Legal Protection for Victims of Artificial Intelligence-Based Pornography in the Form of Deepfakes According to Indonesian Law. *KnE Social Sciences*, **2024**, 265-275.
https://doi.org/10.18502/kss.v8i21.14724

[62] Thing, V.L.L. (2023) Deepfake Detection with Deep Learning: Convolutional Neural Networks versus Transformers. 2023 *IEEE International Conference on Cyber Security and Resilience* (*CSR*), Venice, 31 July-2 August 2023, 246-253.
https://doi.org/10.1109/csr57506.2023.10225004

[63] Mohammed, A. (2024) Deep Fake Detection and Mitigation: Securing Against AI-Generated Manipulation. *Journal of Computational Innovation*, **4**, 1-25.

[64] Lee, G. and Kim, M. (2021) Deepfake Detection Using the Rate of Change between Frames Based on Computer Vision. *Sensors*, **21**, Article 7367.
https://doi.org/10.3390/s21217367

[65] Choi, N. and Kim, H. (2023) DDS: Deepfake Detection System through Collective Intelligence and Deep-Learning Model in Blockchain Environment. *Applied Sciences*, **13**, Article 2122. https://doi.org/10.3390/app13042122

[66] Lee, S.-H., Kwon, K.-R. and Mamunur Rashid, M. (2021) Blockchain Technology for Combating Deepfake and Protect Video/Image Integrity. *Article in Journal of Korea Multimedia Society*, **24**, 1044-1058. https://doi.org/10.9717/kmms.2021.24.8.1044

[67] Hasan, H.R. and Salah, K. (2019) Combating Deepfake Videos Using Blockchain and Smart Contracts. *IEEE Access*, **7**, 41596-41606.
https://doi.org/10.1109/access.2019.2905689

[68] Heidari, A., Navimipour, N.J., Dag, H., Talebi, S. and Unal, M. (2024) A Novel Blockchain-Based Deepfake Detection Method Using Federated and Deep Learning Models. *Cognitive Computation*, **16**, 1073-1091.
https://doi.org/10.1007/s12559-024-10255-7

[69] Maheshwari, R.U. and Paulchamy, B. (2024) Securing Online Integrity: A Hybrid Approach to Deepfake Detection and Removal Using Explainable AI and Adversarial Robustness Training. *Automatika*, **65**, 1517-1532.
https://doi.org/10.1080/00051144.2024.2400640

[70] Wazid, M., Mishra, A.K., Mohd, N. and Das, A.K. (2024) A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, and Societal Impact. *Cyber Security and Applications*, **2**, Article 100040. https://doi.org/10.1016/j.csa.2024.100040

[71] O'Donnell, N. (2021) Have We No Decency? Section 230 and the Liability of Social

Media Companies for Deepfake Videos. *University of Illinois Law Review*, **2021**, 701-740.

[72] Farrell, J. (2024) OpenAI Announces Its New Tool That Can Detect Deepfake Images. Silicon Angle. https://siliconangle.com/2024/05/07/openai-announces-new-tool-can-detect-deepfake-images/

[73] Widder, D.G., Nafus, D., Dabbish, L. and Herbsleb, J. (2022) Limits and Possibilities for "ethical AI" in Open Source: A Study of Deepfakes. 2022 *ACM Conference on Fairness, Accountability, and Transparency*, Seoul, 21-24 June 2022, 2035-2046. https://doi.org/10.1145/3531146.3533779

[74] Socatiyanurak, V., Klangpornkun, N., Munthuli, A., Phienphanich, P., Kovudhikulrungsri, L., Saksakulkunakorn, N., *et al*. (2021) LAW-U: Legal Guidance through Artificial Intelligence Chatbot for Sexual Violence Victims and Survivors. *IEEE Access*, **9**, 131440-131461. https://doi.org/10.1109/access.2021.3113172

[75] Bray, S.D., Johnson, S.D. and Kleinberg, B. (2023) Testing Human Ability to Detect 'Deepfake' Images of Human Faces. *Journal of Cybersecurity*, **9**, tyad011. https://doi.org/10.1093/cybsec/tyad011

[76] McCosker, A. (2022) Making Sense of Deepfakes: Socializing AI and Building Data Literacy on Github and Youtube. *New Media & Society*, **26**, 2786-2803. https://doi.org/10.1177/14614448221093943

[77] King, T.C., Aggarwal, N., Taddeo, M. and Floridi, L. (2019) Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. *Science and Engineering Ethics*, **26**, 89-120. https://doi.org/10.1007/s11948-018-00081-0

[78] Gieseke, A.P. (2020) "The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography. *Vanderbilt Law Review*, **73**, 1479-1515.

[79] Muzykant, V.L., Hossain, B., Muqsith, M.A. and Fatima, M.J. (2022) Media Literacy and Fake News: Bangladesh Perspective. *Jurnal Cita Hukum*, **10**, 223-238. https://doi.org/10.15408/jch.v10i2.25921

[80] Amatika, F. (2022) The Regulation of Deepfakes in Kenya. *Journal of Intellectual Property and Information Technology Law*, **2**, 145-186. https://doi.org/10.52907/jipit.v2i1.208

[81] Anh, N.B.T. (2021) Deepfake and Its Ethics Concerns. Researchgate. https://www.researchgate.net/profile/Anh-Nguyen-Bui/publication/357419167_DEEPFAKE_AND_ITS_ETHICS_CONCERNS/links/61cd5d18d4500608167814ab/DEEPFAKE-AND-ITS-ETHICS-CONCERNS.pdf