Sakarya Üniversitesi
Hukuk Fakültesi Dergisi (SHD)

ISSN 2147-768X

The Sakarya
Journal of Law (The SJL)

Temmuz 2023
C. 11 • S. 1 • s. 701-720

Deepfake Technology: A Criminological Literature Review(*)

Deepfake Teknolojisi: Kriminolojik Bir Literatür Taraması

Fatih ARSLAN(**)

Abstract

Cybercrimes are rapidly evolving with the advancement of technology and reaching new dimensions. Deepfake technology, which is the subject of this article, has also become a part of cybercrime. Deepfake technology, which has similar features to the CGI technology we have encountered in the cinema, is a technology that allows the image or voice of a person - or both - to be transferred to another image or video file in a hyper-realistic way and first came to the agenda in 2017 in social media platform which called as Reddit. Although this technology has many benevolent uses, its malicious use is more prominent. This study aims to compile the criminological studies and current events in the literature on Deepfake for researchers who will study this field in the future. Within the scope of this purpose, the study examines what Deepfake technology is, the methods that can be used to detect Deepfake videos, the criminal dimensions of Deepfake technology and the violations it causes, the characteristics of victims and criminals, and the measures/decisions taken by countries regarding the negative use of Deepfake technology through relevant databases, judicial decisions and newspaper reports.

Keywords

Criminology, Cybercrime, Deepfake, Regulations, Victimology.

(*) Araştırma Makalesi / Makale Geliş Tarihi: 07.05.2023 - Makale Kabul Tarihi: 27.07.2023
DOI: 10.56701/shd.1293642

I would like to thank Prof. Mehmet Tayfun Amman, Assoc. Prof. Nesrin Akıncı Çötok and Salich Tzampaz for their valuable contributions to this article.

(**) Sakarya University, Humanities and Social Sciences Faculty, Sakarya - Türkiye
E-posta: fatih.arslan10@ogr.sakarya.edu.tr
Orcid No: https://orcid.org/0000-0002-9722-2042

Öz

Siber suçlar teknolojinin ilerlemesiyle birlikte hızla gelişmekte ve yeni boyutlara ulaşmaktadır. Bu yazının konusu olan Deepfake teknolojisi de siber suçların bir parçası haline gelmiştir. Sinemada karşılaştığımız CGI teknolojisine benzer özellikler taşıyan Deepfake teknolojisi, bir kişinin görüntüsünün ya da sesinin -ya da her ikisinin birden- hiper-gerçekçi bir şekilde başka bir görüntü ya da video dosyasına aktarılmasını sağlayan bir teknolojidir ve ilk olarak 2017 yılında Reddit isimli bir sosyal medya platformunda gündeme gelmiştir. Bu teknolojinin birçok iyi niyetli kullanımı olsa da kötü niyetli kullanımı daha çok göze çarpmaktadır. Bu çalışma, gelecekte Deepfake teknolojisinin kriminolojik boyutu hakkında çalışacak araştırmacılar için Deepfake üzerine literatürde yer alan kriminolojik çalışmaları ve güncel olayları derlemeyi amaçlamaktadır. Bu amaç kapsamında çalışmada Deepfake teknolojisinin ne olduğu, Deepfake videoların tespitinde kullanılabilecek yöntemler, Deepfake teknolojisinin kriminal boyutları ve neden olduğu ihlaller, mağdurların ve suçluların özellikleri ve Deepfake teknolojisinin olumsuz kullanımına ilişkin ülkelerin aldığı önlemler/kararlar ilgili veritabanları, yargı kararları ve gazete haberleri vasıtasıyla incelenmektedir.

Anahtar Kelimeler

Deepfake, Düzenlemeler, Kriminoloji, Mağdurbilim, Siber Suçlar.

INTRODUCTION

It is possible to see changes in the quality and quantity of crimes as time passes. The technological age we are living in has led to a serious change in the nature of crimes through the opportunities it provides, leading to crimes being committed on the virtual plane rather than the physical plane. The changes it has brought about have enabled it to be evaluated in a different crime category under the concept of cybercrimes. The main distinction between cybercrimes and physical crimes is that cybercrimes take place in the digital environment. However, while physical crimes are evaluated within the framework of physical injuries and property damages, cybercrimes have brought innovations in the nature of the crime such as digital financial robberies and information theft[1]. It is clear today that cybercrime is becoming a serious concern. According to a 2011 study, 74 million people in the US were victims of cybercrime, resulting in direct financial losses of $32 billion[2]. In 2021, this number increased tremendously, causing worldwide damage of 6 trillion dollars, while there are expectations that this damage will reach 10.5 trillion dollars in 2025[3].

Cybercrimes are reaching very different dimensions with the rapidly developing technology. Deepfake technology, which is the subject of this study,

1 Yanping Zhang et al., "A Survey of Cyber Crimes: A Survey of Cyber Crimes," *Security and Communication Networks* 5/4 (April 2012), 422-437.

2 Hemraj Saini et al., "Cyber-Crimes and Their Impacts: A Review," *International Journal of Engineering Research* 2/2 (2012), 202-209.

3 Steve Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," *Cybercrime Magazine* (blog), 2020.

has also become a part of cybercrimes. Deepfake technology, which has similar features to the CGI technology we have come across in cinema, is a technology that allows the image or voice of a person - or both - to be transferred to another visual or video file in a hyper-realistic way and first came to the agenda in 2017. With good intentions, it can provide serious benefits in many fields from education to art, from art to health, and from health to entertainment. However, when used maliciously, it has the potential to negatively affect everything from pornography to violations of personal rights, perception operations, international crises, and even the fate of countries. Taking this potential seriously, international organizations see Deepfake as one of the biggest threats of the future[4]. This study aims to present criminological studies on Deepfake in the literature. It aims to create a holistic compilation for future research in this field by presenting examples from current situations and events.

Within the scope of this purpose, this study examines the nature of Deepfake technology, the methods that can be used to detect videos through Deepfake, the criminal dimensions of Deepfake technology and the violations it causes, the characteristics of victims and criminals, and the measures / senate decisions taken by countries regarding the negative use of Deepfake technology. The method chosen for the realization of this study is document analysis. Document analysis is a systematic procedure for examining or evaluating documents, both printed and electronic (computer-based and internet-transmitted). Like other analytical methods in qualitative research, document analysis requires examining and interpreting data to uncover meaning, gain understanding and develop empirical knowledge[5]. In line with these objectives, the studies, regulations and news on the criminological content of Deepfake since 2017 have been searched in the following databases:

- ProQuest,
- Google Scholar,
- WorldLII,
- LexisNexis,
- WestLaw,
- Web of Science
- Google News

[4] European Union Agency for Law Enforcement Cooperation., *Facing Reality?: Law Enforcement and the Challenge of Deepfakes : An Observatory Report from the Europol Innovation Lab.* (LU: Publications Office, 2022).

[5] Glenn A. Bowen, "Document Analysis as a Qualitative Research Method," *Qualitative Research Journal* 9/2 (August 3, 2009), 27-40.

I. EMERGENCE OF DEEPFAKE

The term Deepfake was first used on a social media platform called Reddit in 2017[6]. This concept is a combination of the words Deep learning and fake. People working in this field used to define Deepfake as the use of artificial intelligence to modify the facial map to create new hyper-realistic images. However, with the development of Deepfake technology, sound, and image can now be produced simultaneously or individually[7].

Deepfake videos are produced through GAN (Generative Adversarial Network) technology used in artificial intelligence[8]. GAN is formed by using two different networks together[9]. The first one is the generator network. The generator network can generate realistic images, sounds and data from noise or vectors. The second network is the discriminator network. This network tries to distinguish between the real data and the fake data produced by the generator. Thus, the discriminator network's correct prediction rate increases, and more realistic images are produced. In other words, GANs are used in the production of media files such as images, audio, and video[10]. This may sound complicated for people who are not very tech-savvy. But today, with a few applications (FaceApp, ReFaceApp, FaceMagic, etc.) that can be downloaded to your smartphones, Deepfake videos can be created with a couple of clicks.

Deepfake technology has positive uses. For example, it can be successfully used for good purposes in the movie industry under the name of CGI. For example, the same character can play the youth or old age of the main character in a scene, or the main character can speak different languages[11]. The positive uses of Deepfake are not limited to cinema. It is also very useful in the fields of education and entertainment. In the field of education, it is possible to make education more fun,

---

6 Matthew B. Kugler - Carly Pace, "Deepfake Privacy: Attitudes and Regulation," *SSRN Electronic Journal* 116/3 (2021), 611-680.

7 Kweilin T. Lucas, "Deepfakes and Domestic Violence: Perpetrating Intimate Partner Abuse Using Video Technology," *Victims & Offenders* 17/5 (July 4, 2022), 647-659; Bahar Uddin Mahmud - Afsana Sharmin, "Deep Insights of Deepfake Technology : A Review," *Dhaka University Journal of Applied Science & Engineering* 2 (2021), 13-23.

8 Peipeng Yu et al., "A Survey on Deepfake Video Detection," *IET Biometrics* 10/6 (November 2021), 607-624.

9 Md Shohel Rana et al., "Deepfake Detection: A Systematic Literature Review," *IEEE Access* 10 (2022), 25494-25513.

10 Md Shohel Rana et al., "Deepfake Detection: A Systematic Literature Review," *IEEE Access* 10 (2022), 25494-25513.

11 Mehmet Emin Masca, "Advantages and Disadvantages of Deepfake Technology," *Geek Culture* (blog), December 3, 2021; Geraint Rees, "Here's How Deepfake Technology Can Be a Good Thing," *World Economic Forum* (November 25, 2019); Mika Westerlund, "The Emergence of Deepfake Technology: A Review," *Technology Innovation Management Review* 9/11 (January 1, 2019), 39-52.

effective and interactive by simulating people's faces and voices[12]. In the field of entertainment, it is also possible to create entertainment in the imitation category by changing faces and voices. An example of this is Mr. Peele's imitation of Barack Obama. Mr. Peele is a very successful comedian and his Barack Obama impersonation made him famous[13]. By using Deepfake technology, he has taken this talent to the next level. In short, the use of Deepfake technology is increasing in many areas from education to art, from health to entertainment.

The fact that Deepfake technology is increasingly being used by ordinary people, rather than experts and people who are aware of the responsibility of this work, paves the way for malicious use and causes us to see Deepfake among the biggest threats of the future. The Deepfake video, which was previously produced for comedic purposes and dealt with a political figure, can lead to international crises, nuclear wars and even the end of the world for humans with malicious use. In an interview with the Wall Street Journal, Hany Farid, an expert on the subject, illustrates this point:

"Imagine the following scenario the video is produced by Donald Trump saying "I've just launched a nuclear weapon against North Korea that video goes on to Twitter and goes viral in 30-60 seconds. North Korea responds in another 60 seconds before anybody figures out that video is fake"[14]

As we have seen, a successful Deepfake video can cause an international crisis in as little as 120 seconds. This is the most extreme example of Deepfake technology being used for malicious purposes, a problem that we will probably never face. But in addition to political problems, Deepfake can also cause a lot of problems on a personal level.

II. DETECTION OF DEEPFAKE CONTENTS

Deepfake technology is producing increasingly realistic images. According to experts in the field, it is not possible to identify a good Deepfake video[15]. example, the TikTok account DeepTomCruise produces content from Deepfake videos produced using Tom Cruise's face[16]. When you watch this person's videos,

12 Simon Chandler, "Why Deepfakes are a Net Positive For Humanity," *Forbes* (2020); Shadrack Awah Buo, "The Emerging Threats of Deepfake Attacks and Countermeasures," (2020).

13 John Fletcher, "Deepfakes, Artificial Intelligence, and Some Kind of Dystopia: The New Faces of Online Post-Fact Performance," *Theatre Journal* 70/4 (2018), 455-471; Cristian Vaccari - Andrew Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News," *Social Media + Society* 6/1 (January 2020), 205630512090340.

14 Wall Street Journal, Deepfake Videos are Getting Real and That's a Problem | Moving Upstream, Youtube, October 15, 2018, https://www.youtube.com/watch?v=Ex83dhTn0IU

15 Mahmud - Sharmin, "Deep Insights of Deepfake Technology : A Review."

16 Shruti Agarwal - Hany Farid, "Detecting Deep-Fake Videos from Aural and Oral Dynamics," *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)* (2021 IEEE/

you may believe that the person in the video is Tom Cruise. This is normal if your eyes are untrained. But for the average technology user, there are a number of things that can help them distinguish Deepfake videos from normal videos.

Table 1. Detection of Deepfake Videos[17]

Deepfake Detection	
- Unnatural Eye Movements - Unnatural Lip Movements - Unnatural Facial Expressions - Difference between skin color tones - Unnatural Body Movement - Awkward-looking body posture - Low Quality	- Awkward Face position with respect to other subjects - The angle formed by the Shadow of the human body - Emotionless Body - Artificial Hair looks - Unnatural Teeth - Non-aligned body parts

As seen in the table above, the things to look out for in detecting moderate Deepfake videos are, in short, anything unnatural in the video. Since the Deepfake video is realized by superimposing another face on top of the original image, pixel shifts are likely to occur. For example, if the person in the original video is looking to the right and the impersonator is looking the other way, this will result in an unnatural eye movement. This can be observed in all other unnatural movements[18].

In Deepfake videos, hair is visually added, so if there is no movement or natural movement of the hair, or if pixels can be seen moving when viewed closely, this can also be a sign of a Deepfake video. Deepfake videos are increasingly being produced in very high quality. However, this can vary depending on the technology used. For example, in Türkiye, a social media influencer allegedly sent a video of himself masturbating to a young girl. This social media influencer was known among his followers as a modest, calm, extremely humble, and very nice person. But after this video hit the internet, he had serious problems. To prove that this video was a Deepfake production, reasons such as the low quality of the video and the presence of an earring in one of the ears were put forward, and the social media influencer was cleared of public accusations.

CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Nashville, TN, USA: IEEE, 2021), 981-989; Rachel Metz, "How a Deepfake Tom Cruise on TikTok Turned into a Very Real AI Company | CNN Business" (2021).

17 This table is based on Mankoo's (2023) study.

18 Sandeep Singh Mankoo, "DeepFakes- The Digital Threat in the Real World," *Gyan Management Journal* 17/1 (2023), 71-77.

III. AS A CRIMINOLOGICAL THREAT "DEEPFAKE"

With its malicious use, Deepfake causes many problems ranging from fraud to violation of personal rights. Mankoo categorized the problems caused by Deepfake under 4 main headings[19].

First, *Sockpuppets*, a term also used in traditional media, refers to a person who does not exist. Sockpuppets are one of the most frequently used methods of fraud. The second is *Politics*. Through the production of Deepfake images, the reputation of politicians can be damaged[20], the fate of elections and even countries can change[21]. Third, *Pornography* is the precursor to the negative use of Deepfake which has made it a societal concern. Every conceivable category can be involved in this type of offense. For example, revenge porn[22], child pornography[23], etc. Scanlon mentioned that over 700k hours of Deepfake videos are uploaded to the internet every day[24]. The last one is *Blackmail*. New images produced through Deepfake can expose innocent people to blackmail. In the next section, I will examine the problems caused by Deepfake through press coverage to help better understand the concepts.

A. FRAUD

You may have experienced or heard of telephone scams before. When you receive a call from a telephone operator or bank with a different number than the customer service number, you are likely to immediately suspect that it is a scam. After all, you don't know the caller and since it's an organization, you can call back in case of a problem. But what if it was the CEO of your company? What would you do if he or she appeared in person, perhaps in an online meeting, with the same voice? This is what happened to a UK-based energy company. By copying the CEO's voice, the scammers called the company's partner firm in Germany and asked them to transfer $243,000 to the account of their supplier in Bulgaria. Claiming that this payment was urgent and the deadline was overdue, the fraudster achieved his goal[25].

---

19 Mankoo, "DeepFakes- The Digital Threat in the Real World."

20 Robert Chesney - Danielle Citron, "Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?" *The Lawfare Blog*, (2018).

21 Bobby Chesney - Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review,* 107/6 (2019).

22 Nicola Henry et al., "Technology-Facilitated Domestic and Sexual Violence: A Review," *Violence Against Women* 26/15-16 (December 2020), 1828-1854.

23 S Eelmaa, "Sexualization of Children in Deepfakes and Hentai," *Trames. Journal of the Humanities and Social Sciences* 26/2 (2022), 229-248.

24 Dr. Thomas P Scanlon, "Data Science & Cybersecurity," *Data Science*, (2023).

25 Jesse Damiani, "A Voice Deepfake Was Used to Scam a CEO Out of $243,000," *Forbes* (2019).

In 2020, the manager of a bank in Hong Kong was called and asked by a familiar voice to approve a $35 Million transfer for an acquisition. Transactions then began to take place through a retained lawyer. Ultimately, $400,000 in stolen money and transfers to other accounts resulted in robberies through the United Arab Emirates[26].

Another example of fraud comes from the family factor, which perhaps most people cannot escape. Imagine that one day your son or daughter calls you on the phone. Your child asks you for money because they are in a very difficult financial situation. You think it is your child with the same voice, the same facial expressions, and everything, but the reality is very different. The Canadian family targeted by fraudsters sent 10,000 dollars to people they thought their children, and the fraudsters reached their target[27].

While fraud is already a serious problem, it seems that Deepfake technology is causing an even more serious problem as it contributes greatly to the most important factor in fraud: credibility. In 2023, Redins wrote that 26 percent of small companies and 38 percent of large companies suffered more than 50 identity fraud attacks in 2022, resulting in losses of up to $480,000[28]. Marks, writing in 2023, noted that last year, damage through impersonated voices amounted to $11 million[29].

B. CYBERBULLYING

Cyberbullying is another crime that can be committed through Deepfake. The scope of cyberbullying is very wide and its effects are quite high. The ability to edit a person's face into a video or image that has nothing to do with them facilitates the use of Deepfake technology in the field of cyberbullying. People can be blackmailed with new images obtained using Deepfake, and their reputation in the social and institutional sphere can be shaken.

In 2021, a woman allegedly used multiple images of girls on a school cheerleading squad to create Deepfake images of herself naked, drinking alcohol and vaping. At the same time, the suspect allegedly harassed these girls by texting them with a phone number obtained from the internet[30]. In 2023, a student

---

26 Thomas Brewster, "Fraudsters Cloned Company Director's Voice in $35 Million Bank Heist, Police Find," *Forbes* (2021).

27 Mark Quinn, "N.L. Family Warns Others Not to Fall Victim to the Same Deepfake Phone Scam That Cost Them $10K | CBC News," *CBC* (2023).

28 | Larisa Redins, "Surprise! Deepfake Fraud on the Rise | Biometric Update" (April 27, 2023).

29 Gene Marks, "It Sounds like Science Fiction but It's Not: AI Can Financially Destroy Your Business," *The Guardian* (April 9, 2023), sec. Business.

30 BBC, "Mother 'Used Deepfake to Frame Cheerleading Rivals,'" *BBC News* (March 15, 2021), sec. Technology.

allegedly uploaded Deepfake nude images of his teacher online and tried to sell them. Although the institution denied the student's guilt, the seriousness of the situation is obvious, no matter who did it[31].

C. DATA MANIPULATION

Deepfake technology can mislead the public by manipulating media files. The potential dangers of this situation are frequently mentioned by academics working in the field. According to academics, media files created through Deepfake can jeopardize the course of elections, reduce trust in institutions, and be used as weapons to create national and international crises. As mentioned above, a successful Deepfake video can cause a nuclear war in 120 seconds. However, there are a couple of cases where hypothetical examples have come true.

On February 24, 2022, Russian forces began their invasion of Ukraine. A video circulated while the war was going on provided an example of the use of Deepfake technology even on the battlefield. In the video, Ukrainian president Volodymyr Zelensky said that Russian soldiers had won the war, Ukraine had given up and the soldiers should lay down their arms. However, this video was soon confirmed to be fake. But a more successful Deepfake video could have caused bigger problems and changed the course of the war.

Deepfake may not only involve political figures and political malevolence. Scholars in the field are also concerned about the use of Deepfake technology to produce pornographic content. This has been one of the most researched topics on the criminological dimension of Deepfake. Today, 96% of Deepfake videos produced contain pornographic content. Celebrities such as Gal Gadot and Scarlet Johansson have had an unfortunate encounter with the negative side of this technology[32]. But the danger is not limited to celebrities and politicians. Noelle Martin begins a TED talk by asking the question "Have you ever Googled yourself?"[33]. For Noelle Martin, the nature of this question is as follows. After Googling herself, Martin saw her own face in a porn video. This painful experience makes many people ask themselves whether they too have been victims of this crime. In addition, on April 18, 2023, it was reported that a suspect named Patrick Carey manipulated the images of his former schoolmates under the age of 18 through Deepfake technology to produce sexual content. The suspect who

31 MaryAnn Martinez, "Texas Teacher Latest Victim of Deepfake Nude Pics," 2023.

32 Marie-Helen Maras - Alex Alexandrou, "Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos," *The International Journal of Evidence & Proof* 23/3 (July 2019), 255-262.

33 Wall Street Journal, Deepfake Videos are Getting Real and That's a Problem | Moving Upstream, Youtube, October 15, 2018, https://www.youtube.com/watch?v=Ex83dhTn0IU

published these images on a website was caught 2 years after the incident and sentenced to 6 months in prison[34].

As seen, data manipulation through Deepfake leads to many violations of personal rights. By means of Deepfake technology, another person can register on your behalf on financial sites where you register with your identity and photographs, and this can lead to serious financial losses.

D. FALSE TESTIMONY

Another problem created by the malicious use of deepfake technology is perjury. Today, many legal experts are discussing this issue intensively. Deepfake technology can produce active images. This enables the production of misleading evidence[35]. Today, video and audio recordings are very valuable in the legal system. However, media files that can be produced through Deepfake can be presented as evidence in courts, leading to the punishment of innocent people. Deepfake technology may become one of the biggest dangers awaiting the legal systems of countries that are not sufficiently aware of it. Or, as Sawan & Sawan put it, "Thus, the justice that is sought can just go out of the window with a click of the play button"[36].

IV. CHARACTERISTICS OF VICTIMS AND OFFENDERS

As the area of use of Deepfake technology expands and the number of users increases, its victims diversify at the same rate. In other words, Deepfake can victimize anyone in a literal sense. However, there is generally a reason why the victimized person is targeted due to the malicious origin of the victimization. The characteristics of the victims of Deepfake, which generally lead to scandalous incidents, are as follows:

Popular and well-known people are those who are constantly in the public eye and periodically appear on the agenda of society. This is a sought-after situation for those who use Deepfake technology maliciously. The images produced using the faces and voices of these people have a damage network that ranges from simple entertainment to the pornography industry.

Young women, young women are seen as a disadvantaged group in almost all areas of research in criminology. The possibilities provided by deepfake

---

[34] Dennis A Clark - Priscilla DeGregory, "Patrick Carey Gets 6 Months for Posting Deepfake Pics of Underage Girls on Porn Sites" (2023).

[35] Matthew B. Kugler - Carly Pace, "Deepfake Privacy: Attitudes and Regulation," *SSRN Electronic Journal* 116/3 (2021), 611-680.

[36] Sawan & Sawan, "Deepfake Videos as Evidence in Court - Sawan & Sawan LLC | Trial Lawyers," *Sawan and Sawan - Injury Lawyers* (blog), January 27, 2020.

technology can target a perfectly normal person, as seen in the example news reports above. In another news report, people who can use this technology can harm young women for revenge or for personal gratification. It is worth noting that 96% of Deepfake victims are women[37]. According to another study cited by Berk, it is seen that the victims of Deepfake videos on porn sites are all women, while on Youtube, men are more targeted with a rate of 61%[38].

Political figures, those who govern the country or are candidates for governance are constantly battling armies of trolls and unfounded news about them. Fighting some allegations can be very tiring at times. Especially at critical times, such as election times, old files are constantly opened and politicians are targeted. By manipulating media files, deepfake technology can permanently damage their reputation.

Business Leaders, as exemplified by previous news stories, companies can suffer major financial damage through media files produced by copying the voices and images of business leaders. It is therefore very likely that professional theft gangs will target business leaders when using Deepfake.

Articles written about the criminological dimension of Deepfake always talk about the victims or the damage that Deepfake has caused or could cause. If we accept that Deepfake is one of the biggest threats that awaits us in the future, it is important to know what and who we are up against. When the news and court records related to Deepfake are analyzed, it is seen that the suspects have the following characteristics.

Articles written about the criminological dimension of Deepfake always talk about the victims or the damage that Deepfake has caused or could cause. If we accept that Deepfake is one of the biggest threats that awaits us in the future, it is important to know what and who we are up against. When the news and court records related to Deepfake are analyzed, it is seen that the suspects have the following characteristics.

- 15-25 years old
- Socially and mentally challenged
- Having unsupervised parents

The main reason why the suspects are 15-25 years old is that new technologies are used and preferred especially by young people aged 15-25. In her study, Suvurova identifies Deepfake pornography with Jenkins' participatory culture[39].

37 Henry Ajder et al., "The State of Deepfakes: An Overview," *Deeptrace*, (2017), 1-20.

38 Mustafa Evren Berk, "Dijital Çağın Yeni Tehlikesi 'Deepfake,'" *OPUS Uluslararası Toplum Araştırmaları Dergisi* 16/28 (August 31, 2020), 1508-1523.

39 Inna Suvorova, "Deepfake Pornography as a Male Gaze on Fan Culture," (2022).

According to Suvurova, participatory culture has five main characteristics: relatively unhindered artistic and civic participation, encouragement of people to share their creations, informal mentoring based on the exchange of experience, individuals who feel their contributions are important, and members who feel a social connection. Social media platforms such as Reddit are a home for all the main features mentioned by Jenkins.

When cybercrimes, especially stalking, are examined, we can see that people are mentally and socially troubled. In a news article in the New York Post, the suspect described himself as socially and mentally problematic[40]. It is possible that this is a fabrication by the suspect. However, in the WSJ reporter's interview with a person who produces harmful content through Deepfake, the interviewee's lack of empathy is striking. According to this person, the people harmed by Deepfake videos do not matter.

Since there are no psychology studies conducted on suspects in the field, it is difficult to draw more detailed conclusions. However, people who do not have such problems and who commit fraud professionally have similar characteristics with those in the cyber fraudster category.

V. LEGAL REGULATIONS WORLDWIDE

Today we can clearly see that Deepfake technology is also seen as a serious problem by countries. Many countries have introduced new regulations on Deepfake or expanded the scope of old regulations. Many countries that have not taken concrete steps for legal regulations are also preparing for concrete steps. However, in this section, the legal regulations introduced or committed by countries that have taken direct steps to combat Deepfakes or have made official statements that they will do so will be discussed.

A. UNITED STATES OF AMERICA

Several states in the United States are leading the way in reforming Deepfakes. On May 18, 2021, the state of New York amended its law on the detection of harassment through electronic and digital communications to provide victims with a private right of action to track and prevent the illegal dissemination of Deepfake content, according to a senate resolution passed on May 18, 2021. In addition, under this law, those who harass and blackmail people through illegally produced Deepfake images will be prosecuted for felony harassment (S 6829A).

According to the State of Hawaii's decision, the production of Deepfake videos, threatening or exposing a person through such videos constitutes a

[40] Clark - DeGregory, "Patrick Carey Gets 6 Months for Posting Deepfake Pics of Underage Girls on Porn Sites" (2023).

violation of the right to privacy in the first degree. The 21st Century Privacy Law Task Force, established in 2019, also recommended that states swiftly pass legislation aimed at combating Deepfake (SB 2292).

With the widespread use of Deepfake technology, the State of Georgia has also revised old legal regulations. Accordingly, persons who distribute and maliciously use images produced through Deepfake will be deemed to be guilty of a gross misdemeanor, punishable by imprisonment from 1 year to 5 years or a fine of not more than $100,000 (SB 78).

The Senate of the State of New Jersey in 2020 passed a bill aimed at securing elections. According to this decision, Deepfake videos produced to damage the reputation of candidates during election times will be criminalized. However, according to this law, videos with humorous purposes will be excluded from this scope (AB 4985).

The law of the State of Texas, enacted in 2023, aims to prevent the targeting of young people under the age of 18 through Deepfake videos. According to this law, using people's faces and images to create pornographic images will be criminalized as of 2023 (HB 2700).

The State of California has enacted 2 different laws to address both the sexual and political aspects of Deepfake technology. AB 602 stands against media files with pornographic content produced without the consent of individuals. AB 730 was enacted to ensure the security of the electoral process. This bill would prohibit, until January 1, 2023, a person, committee, or other entity from distributing, within 60 days of an election in which a candidate is on the ballot, materially deceptive audio or visual media of the candidate to discredit the candidate or deceive a voter into voting for or against the candidate, unless the media contains a statement that the media was manipulated.

B. CHINA

China has introduced very strict new provisions on the use of Deepfake technology. However, the provisions directly target the artificial intelligence companies that are instrumental in the production of Deepfake images. According to the provisions adopted by the CAC, any content produced using an AI system must bear the watermark of the program from which the content was produced and must be annotated. AI companies providing these services must undertake not to process personal data. However, companies should also consider processes such as the verification of user identities[41]. Hine and Floridi have argued that these

[41] CAC, "国家互联网信息办公室等三部门发布《互联网信息服务深度合成管理规定》-中共中央网络安全和信息化委员会办公室" (2022); Asha Hemrajani, "China's New Legislation on Deepfakes: Should the Rest of Asia Follow Suit?" (2023).

regulations could restrict people's online freedoms in China[42]. Of course, these provisions may harm people's lives by causing restrictions, but it is important to remember that freedoms can cause as much harm as restrictions.

C. UNITED KINGDOM

The UK is also highly vulnerable to the harms of Deepfake. In the UK, 1 in 14 adults are at risk of having inappropriate images of themselves spread online. From 2015 to 2021, there were 28,000 complaints of non-consensual sexual content recorded in police reports[43]. To address this problem seriously, the UK aims to enact the Online Safety Bill. This law will have a wide scope in terms of content, from pornography to political content[44]. It is also envisaged that suspects will be imprisoned under this law. However, it should be noted that this law has not yet come into force. Therefore, we do not have more information.

According to the pie chart in the conclusion section of the study by Firc et al., it is seen that the majority of searches for the word "deepfake" between 2021 and 2022 originated from the USA and China[45] Not surprisingly, the most serious steps taken against the malicious use of deepfake technology are also coming from the USA and China. In the rest of the world, although Deepfake technology is not directly mentioned, some laws refer to such situations. For example, the Turkish Criminal Code (TCK art. 267/1) has regulations on the fabrication of images to be used for slander[46]. However, although many countries such as Türkiye[47] and Australia[48] have expressed their concerns on this issue, it is seen that they have not taken a concrete step directly on Deepfake crimes.

CONCLUSION

The use of deepfake technology is on the rise. Moreover, this increase is not only among experts or responsible people working in the field but also among

---

42 Emmie Hine - Luciano Floridi, "New Deepfake Regulations in China are a Tool for Social Stability, but at What Cost?," *Nature Machine Intelligence* 4/7 (July 20, 2022), 608-610.

43 GOV UK, "New Laws to Better Protect Victims from Abuse of Intimate Images," *GOV.UK* (2022).

44 Monika Plaha - Joseph Lee, "Sharing Pornographic Deepfakes to Be Illegal in England and Wales," *BBC News* (November 25, 2022), sec. Technology.

45 Anton Firc et al., "Deepfakes as a Threat to a Speaker and Facial Recognition: An Overview of Tools and Attack Vectors," *Heliyon* 9/4 (April 2023), e15090.

46 Beşir Babayiğit, "Deepfake'in Ceza Hukuku Bakımından Değerlendirilmesi ve De Lege Ferenda Öneriler," *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, (November 4, 2021), 655-703.

47 Elif Karakoç - Burcu Zeybek, "Görmek İnanmaya Yeter Mi? Görsel Dezenformasyonun Ayırt Edici Biçimi Olarak Siyasi Deepfake İçerikler," *Öneri Dergisi* 17/57 (August 25, 2021), 50-77.

48 Federica Celli, "Deepfakes are Coming: Does Australia Come Prepared?," *Canberra Law Review* 17/2 (2020), 193-204.

ordinary people. This characteristic of the situation makes it difficult to control Deepfake technology and may increase the number of victims and the potential damage that can be done in general. For example, as seen in the news report above, the problem caused to other girls on the same cheerleading squad as her daughter because the girl's mother was able to use Deepfake technology illustrates the severity of the situation. In Table 1 above, I have listed many ways in which Deepfake videos can be detected by normal people, and according to the table, any unnatural movement can potentially indicate Deepfake content. However, for those who do not have a basic level of knowledge about Deepfake, it will not be easy to detect the relevant content. The negative use of Deepfake technology can lead to many financial, psychological, legal, and political problems. Financially, successful Deepfake content can mean the end of your company. Psychologically, you may face problems such as depression and suicidal tendencies. Legally, fake evidence produced through Deepfake technology can lead to you being declared guilty. Politically, Deepfake technology can change the course of elections and cause international crises.

Another aspect related to Deepfake technology is the characteristics of victims and criminals. Victims are, to summarize very briefly, people worth victimizing[49]. This may seem like a very harsh statement at first reading, but I think this statement will be justified when the news I have shared above and the sources in the literature are examined. Nevertheless, victims are women, politicians, celebrities, public figures, and business leaders. Anyone can, of course, become the content of a Deepfake video, as I mentioned earlier. But according to the current literature, the targeted people have the listed characteristics. One of the main problems in cybercrime is that almost 90% of criminals are not caught[50]. The 3 characteristics of those who use Deepfake technology for criminal purposes, which are mentioned based on captured criminals, are not based on any field research. This can be said to be one of the most important gaps in the literature. Criminals can be profiled more clearly through psychological research in this field.

When the relevant literature is examined, a serious deficiency is observed. This deficiency stems from the fact that the topic under study is relatively new and does not have a clear sample. To clarify what is meant by a clear sample, it can be said as follows. In Deepfake-related crimes, many of the victims may not even be aware that they are victims. However, the sample that is the source of the problems is very difficult to reach or unknown. This situation weakens the effectiveness of social scientists in developing solutions.

[49] This expression refers to the journalistic term "newsworthy". It refers to the rational cost-benefit thinking in the targeting of suspects.

[50] Zhang et al., "A Survey of Cyber Crimes."

Another problem is that the studies conducted in the field are only aimed at revealing the current situation since the related subject is quite new. As the related literature develops, it is possible to observe a significant increase in studies aimed at solving the problems related to this issue. However, the current situation did not have enough infrastructure for solution proposals.

But in spite of everything, governments are working to prevent and reduce the negative consequences of Deepfake. These efforts are realized through new draft laws or the revision of old ones. Today, it seems that the Chinese Government has the most stringent solution to this problem. Today, many states in the US do not seem to have addressed this issue. In the current situation, the legal systems of countries that do not address this problem sufficiently can be abused by criminals who take advantage of this situation.

REFERENCES

Agarwal, Shruti - Farid, Hany. "Detecting Deep-Fake Videos from Aural and Oral Dynamics." *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. 981-989. Nashville, TN, USA: IEEE, 2021. https://doi.org/10.1109/CVPRW53098.2021.00109

Ajder, Henry et al. "The State of Deepfakes: An Overview." *Deeptrace*, 1-20.

Babayiğit, Beşir. "Deepfake'in Ceza Hukuku Bakımından Değerlendirilmesi ve De Lege Ferenda Öneriler." *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 655-703. https://doi.org/10.34246/ahbvuhfd.1018877

BBC. "Mother 'Used Deepfake to Frame Cheerleading Rivals.'" *BBC News* (March 15, 2021), sec. Technology. https://www.bbc.com/news/technology-56404038

Berk, Mustafa Evren. "Dijital Çağın Yeni Tehlikesi 'Deepfake.'" *OPUS Uluslararası Toplum Araştırmaları Dergisi* 16/28 (August 31, 2020), 1508-1523. https://doi.org/10.26466/opus.683819

Bowen, Glenn A. "Document Analysis as a Qualitative Research Method." *Qualitative Research Journal* 9/2 (August 3, 2009), 27-40. https://doi.org/10.3316/QRJ0902027

Brewster, Thomas. "Fraudsters Cloned Company Director's Voice in $35 Million Bank Heist, Police Find." *Forbes*. 2021. Accessed May 1, 2023. https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/

CAC. "国家互联网信息办公室等三部门发布《互联网信息服务深度合成管理规定》-中共中央网络安全和信息化委员会办公室." 2022. Accessed May 2, 2023. http://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm

Celli, Federica. "Deepfakes are Coming: Does Australia Come Prepared?" *Canberra Law Review* 17/2 (2020), 193-204.

Chandler, Simon. "Why Deepfakes are a Net Positive for Humanity." *Forbes*. 2020. Accessed May 1, 2023. https://www.forbes.com/sites/simonchandler/2020/03/09/why-deepfakes-are-a-net-positive-for-humanity/

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

Chesney, Robert - Citron, Danielle. "Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?" *The Lawfare Blog*.

Clark, Dennis A - DeGregory, Priscilla. "Patrick Carey Gets 6 Months for Posting Deepfake Pics of Underage Girls on Porn Sites." 2023. Accessed May 1, 2023. https://nypost.com/2023/04/18/ny-man-patrick-carey-gets-6-months-for-posting-deepfaked-pics-on-porn-sites/

Damiani, Jesse. "A Voice Deepfake Was Used to Scam a CEO Out of $243,000." *Forbes*. 2019. Accessed May 1, 2023. https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/

Eelmaa, S. "Sexualization of Children in Deepfakes and Hentai." *Trames. Journal of the Humanities and Social Sciences* 26/2 (2022), 229-248. https://doi.org/10.3176/tr.2022.2.07

European Union Agency for Law Enforcement Cooperation. *Facing Reality?: Law Enforcement and the Challenge of Deepfakes : An Observatory Report from the Europol Innovation Lab.* LU: Publications Office, 2022. https://data.europa.eu/doi/10.2813/08370

Firc, Anton et al. "Deepfakes as a Threat to a Speaker and Facial Recognition: An Overview of Tools and Attack Vectors." *Heliyon* 9/4 (April 2023), e15090. https://doi.org/10.1016/j.heliyon.2023.e15090

Fletcher, John. "Deepfakes, Artificial Intelligence, and Some Kind of Dystopia: The New Faces of Online Post-Fact Performance." *Theatre Journal* 70/4 (2018), 455-471. https://doi.org/10.1353/tj.2018.0097

GOV UK. "New Laws to Better Protect Victims from Abuse of Intimate Images." *GOV. UK*. 2022. Accessed May 2, 2023. https://www.gov.uk/government/news/new-laws-to-better-protect-victims-from-abuse-of-intimate-images

Hemrajani, Asha. "China's New Legislation on Deepfakes: Should the Rest of Asia Follow Suit?" 2023. Accessed May 2, 2023. https://thediplomat.com/2023/03/chinas-new-legislation-on-deepfakes-should-the-rest-of-asia-follow-suit/

Henry, Nicola et al. "Technology-Facilitated Domestic and Sexual Violence: A Review." *Violence Against Women* 26/15-16 (December 2020), 1828-1854. https://doi.org/10.1177/1077801219875821

Hine, Emmie - Floridi, Luciano. "New Deepfake Regulations in China are a Tool for Social Stability, but at What Cost?" *Nature Machine Intelligence* 4/7 (July 20, 2022), 608-610. https://doi.org/10.1038/s42256-022-00513-4

Karakoç, Elif - Zeybek, Burcu. "Görmek İnanmaya Yeter Mi? Görsel Dezenformasyonun Ayırt Edici Biçimi Olarak Siyasi Deepfake İçerikler." *Öneri Dergisi* 17/57 (August 25, 2021), 50-77. https://doi.org/10.14783/maruoneri.908542

Kugler, Matthew B. - Pace, Carly. "Deepfake Privacy: Attitudes and Regulation." *SSRN Electronic Journal* 116/3 (2021), 611-680. https://doi.org/10.2139/ssrn.3781968

Kugler, Matthew B. - Pace, Carly. "Deepfake Privacy: Attitudes and Regulation." *SSRN Electronic Journal* 116/3 (2021), 611-680. https://doi.org/10.2139/ssrn.3781968

Lucas, Kweilin T. "Deepfakes and Domestic Violence: Perpetrating Intimate Partner Abuse Using Video Technology." *Victims & Offenders* 17/5 (July 4, 2022), 647-659. https://doi.org/10.1080/15564886.2022.2036656

Mahmud, Bahar Uddin - Sharmin, Afsana. "Deep Insights of Deepfake Technology : A Review." *Dhaka University Journal of Applied Science & Engineering* 2 (2021), 13-23.

Mankoo, Sandeep Singh. "DeepFakes- The Digital Threat in the Real World." *Gyan Management Journal* 17/1 (2023), 71-77. https://doi.org/10.48165/gmj.2022.17.1.8

Maras, Marie-Helen - Alexandrou, Alex. "Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos." *The International Journal of Evidence & Proof* 23/3 (July 2019), 255-262. https://doi.org/10.1177/1365712718807226

Marks, Gene. "It Sounds like Science Fiction but It's Not: AI Can Financially Destroy Your Business." *The Guardian* (April 9, 2023), sec. Business. https://www.theguardian.com/business/2023/apr/09/it-sounds-like-science-fiction-but-its-not-ai-can-financially-destroy-your-business

Martinez, MaryAnn. "Texas Teacher Latest Victim of Deepfake Nude Pics," 2023. https://nypost.com/2023/04/14/texas-student-faked-nudes-of-teacher-report/

Masca, Mehmet Emin. "Advantages and Disadvantages of Deepfake Technology." *Geek Culture* (blog), December 3, 2021. https://medium.com/geekculture/advantages-and-disadvantages-of-deepfake-technology-ccfa7c12b1ae

Metz, Rachel. "How a Deepfake Tom Cruise on TikTok Turned into a Very Real AI Company | CNN Business." 2021. Accessed May 1, 2023. https://edition.cnn.com/2021/08/06/tech/tom-cruise-deepfake-tiktok-company/index.html

Morgan, Steve. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." *Cybercrime Magazine* (blog), 2020. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Plaha, Monika - Lee, Joseph. "Sharing Pornographic Deepfakes to Be Illegal in England and Wales." *BBC News* (November 25, 2022), sec. Technology. https://www.bbc.com/news/technology-63669711

Quinn, Mark. "N.L. Family Warns Others Not to Fall Victim to the Same Deepfake Phone Scam That Cost Them $10K | CBC News." *CBC*. 2023. Accessed May 1, 2023. https://www.cbc.ca/news/canada/newfoundland-labrador/deepfake-phone-scame-1.6793296

Rana, Md Shohel et al. "Deepfake Detection: A Systematic Literature Review." *IEEE Access* 10 (2022), 25494-25513. https://doi.org/10.1109/ACCESS.2022.3154404

Rana, Md Shohel et al. "Deepfake Detection: A Systematic Literature Review." *IEEE Access* 10 (2022), 25494-25513. https://doi.org/10.1109/ACCESS.2022.3154404

Redins, | Larisa. "Surprise! Deepfake Fraud on the Rise | Biometric Update." April 27, 2023. Accessed May 1, 2023. https://www.biometricupdate.com/202304/surprise-deepfake-fraud-on-the-rise

Rees, Geraint. "Here's How Deepfake Technology Can Actually Be a Good Thing." *World Economic Forum*. November 25, 2019. Accessed May 1, 2023. https://www.weforum.org/agenda/2019/11/advantages-of-artificial-intelligence/

Saini, Hemraj et al. "Cyber-Crimes and Their Impacts: A Review." *International Journal of Engineering Research* 2/2 (2012), 202-209.

Sawan, Sawan &. "Deepfake Videos as Evidence in Court - Sawan & Sawan LLC | Trial Lawyers." *Sawan and Sawan - Injury Lawyers* (blog), January 27, 2020. https://sawanandsawan.com/deepfake-videos-as-evidence-in-court/

Scanlon, Dr Thomas P. "Data Science & Cybersecurity." *Data Science*.

Shadrack Awah Buo. "The Emerging Threats of Deepfake Attacks and Countermeasures." https://doi.org/10.13140/RG.2.2.23089.81762

Suvorova, Inna. "Deepfake Pornography as a Male Gaze on Fan Culture."

Vaccari, Cristian - Chadwick, Andrew. "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News." *Social Media + Society* 6/1 (January 2020), 205630512090340. https://doi.org/10.1177/2056305120903408

Westerlund, Mika. "The Emergence of Deepfake Technology: A Review." *Technology Innovation Management Review* 9/11 (January 1, 2019), 39-52. https://doi.org/10.22215/timreview/1282

Yu, Peipeng et al. "A Survey on Deepfake Video Detection." *IET Biometrics* 10/6 (November 2021), 607-624. https://doi.org/10.1049/bme2.12031

Zhang, Yanping et al. "A Survey of Cyber Crimes: A Survey of Cyber Crimes." *Security and Communication Networks* 5/4 (April 2012), 422-437. https://doi.org/10.1002/sec.331.