Turk. J. Math. Comput. Sci.
18(2)(2026) 461–480
© MatDer
DOI : 10.47000/tjmcs.1823208

Fake Truths, Real Harm: Analytical Approaches to Deepfakes and Personal Data Breach

Zeynep Hazal GÜNAY[1,*], Mustafa ALKAN[2]

[1]*Department of Computer Forensics, Informatics Institute, Gazi University, Ankara, Türkiye.*
[2]*Department of Electrical and Electronics Engineering, Faculty of Technology, Gazi University, Ankara, Türkiye.*

Received: 13-11-2025 • Accepted: 28-12-2025

Abstract. Deepfake technology, a product of rapid advances in artificial intelligence, enables the creation of hyper-realistic synthetic content depicting events that never occurred. While offering many beneficial usages in areas like education, culture, health and accessibility, it also possesses a serious risk such as disinformation, blackmail, fraud, and identity theft, threatening cybersecurity and personal data protection. As there is currently no specific legal framework regulating Deepfakes in Türkiye, this study examines their associated risks, personal data vulnerabilities, notable cases, international approaches, and proposes recommendations to support effective mitigation in Türkiye.

2020 AMS Classification: 68P27, 68T07

Keywords: Deepfake, personal data, cybersecurity, information security.

1. Introduction

One of the most significant innovations that rapidly advancing technology has brought into our lives is artificial intelligence (AI) systems, which enable a wide range of tasks -from everyday activities to professional operations- to be carried out within seconds. Thanks to the developments in AI, particularly in the fields of Deep Learning (DL) and Machine Learning (ML), synthetic content generation has become possible within seconds through applications that require no specialized expertise and are often offered as free services. In this context, Deepfake algorithms have emerged as a type of Deep Learning algorithm that enables the production of highly realistic audio, visual, video and textual content, depicting events that never occurred. Such content can be used as a tool in various beneficial applications across domains such as education, culture, arts, psychology, healthcare, accessibility, and advertising. Despite these positive use areas, Deepfake technologies also possess a significant potential to be exploited for malicious or criminal purposes. Studies indicate that by 2026, approximately 90% of all online content may be synthetically generated, which highlight the growing threat posed by malicious Deepfakes [60].

The term Deepfake is a portmanteau derived from the combination of “deep”, representing DL algorithms that from the core of its architecture, and “fake” symbolizing fabricated media. The concept first appeared in 2017 as the pseudonym of a Reddit user who produced and disseminated non-consensual intimate videos featuring woman celebrities. Subsequently, the term came to denote all similar synthetically produced content [82].

*Corresponding Author
Email addresses: gunayzeynephazal@gmail.com (Z.H. Günay), alkan@gazi.edu.tr (M. Alkan),



FIGURE 1. Istanbul landscape as if it had been painted by Pablo Picasso (Created with Gemini AI)

Although numerous definitions of Deepfake exist in academic literature, there is no single, universally accepted and comprehensive definition of the concept. In a recent study reviewing 79 academic papers with 61 definitions of Deepfake were analysed, most focused primarily on video and image-based content, while far fewer addressed *text* Deepfakes [11]. In some cases, Deepfakes are created entirely from scratch to depict actions or events that never occurred, while in other instances, manipulation of existing media is sufficient to achieve the intended effect.

A term frequently conflated with Deepfakes in the literature is **synthetic media**. This *chapeau* term encompasses all artificially generated content, including Deepfakes [28]. Deepfake media, however, constitutes a specific subset of synthetic media-referring to content that closely resembles real people, objects, or events, often with the deliberate intent of persuading viewers of its authenticity. For instance, an AI-generated painting depicting an Istanbul landscape *as if it had been painted by Pablo Picasso* (Figure 1.) would qualify as an example of synthetic media. In this case, the content is synthetic but not deceptive- it does not portray a fabricated event or person, nor is its persuasive realism of particular importance. Rather, it exemplifies the broader class of artificially generated media. By contrast, the synthetic generation of content depicting a clearly identifiable, real individual -such as Pablo Picasso, again - engaging in an action he has never actually performed, for instance, painting Figure 1 would be classified as a Deepfake (Figure 2).

Generation of Deepfakes depends on collecting target data and training models based on that data. This process can create various vulnerabilities in terms of **information security**, and **cybersecurity**, both during the acquisition of **training data**, **content creation** and during the **dissemination** of the generated content. In particular, the use of biometric data -such as voice and facial features- belonging to identifiable real individuals requires special sensitivity with regard to consent and protection. Even when the creation and use of Deepfake content are not aimed for criminal purposes, the process of collecting, processing, storing and distributing **personal data** raise significant concerns.

2. DEEPFAKE GENERATION

DL represents a revolutionary field within AI, characterized by the use of nested non-linear structures often in form of Deep Neural Networks (DNNs) which are an advanced form of Artificial Neural Networks (ANNs). The core mechanisms involve composing single modules that iteratively transform the data representation to a higher, more abstract level. By the use of massive datasets, such as ImageNet, and advances in methodology, these models have allowed AI systems to match or surpass human performance on complex tasks, including image classification and speech understanding.



FIGURE 2. Image depicting Pablo Picasso painting Figure 1. (Created with Gemini AI)

The approach on creating Deepfakes usually depends on the content type. According to first-quarter 2025 data, video-based Deepfake content represents the largest share of synthetic media, accounting for 46% of total output, followed by image-based content at 32%, and audio-based content at 22% [68].

Deepfake generation approaches can be divided into two as *algorithms* and *techniques*. Algorithms, learns statistics of the input data for mathematical synthesis of new content, while techniques are built around the algorithms to achieve specific goals like "Face Swapping".

2.1. **Core Deepfake Algorithms.** There are various approaches to generate a Deepfake content. One of the most prevalent methods, with origins dating back to 2014, is the ***Generative Adversarial Networks (GAN)***. Within a GAN, the "**generator**" neural network is trained on target data to learn its features, enabling the creation of new examples that mimic the original data's characteristics. The generated samples are then evaluated by a second neural network, the "**discriminator**" which identifies and rejects sample that do not sufficiently resemble authentic data. The greater the volume and quality of original training data, the more realistic the resulting outputs tend to be. As training progress, the adversarial tension between the two networks gradually stabilizes, resulting in a generator capable of producing increasingly realistic examples and a discriminator capable of performing more refined analyses [82]. However, GANs are difficult to train due to the adversarial balance between the two neural networks, which can lead to training instability or "**mode collapse**", where the Generator starts producing a limited variety of output to easily fool the Discriminator [48]. Basic working architecture of a GAN be seen in the Figure 3.

Autoencoders (AEs) are another core algorithm that enables to produce Deepfakes. Autoencoders are neural networks, designed for **compression** and **reconstruction** and built on "**encoder**" and "**decoder**". Encoder consists of layers that progressively narrow, and the Decoder consists of layers that progressively widen back to original input size. The network is trained on a self-supervised task of reconstructing exact same points it is fed through the latent space [90]. Variational Autoencoder (VAE) enhances the concept to another level by adding *latent probabilistic distributions*. Unlike basic autoencoders, VAEs not only can reconstruct the input data accurately, but also can generate new samples that resembles the original input [9]. Figure 4 presents basic working architecture of a VAE. Input data -an image for example- is fed to an encoder to result in a *latent space* which can be summarized as a lower dimensional representation of the original input. Decoder takes the latent face to reconstruct the input from its core features.

VAEs produce lossy outputs while GANs not, GANs are hard to train while VAEs not, the two core algorithms both have cons and pros and followed by a relatively new, highly sophisticated approach "**Diffusion Models**". Diffusion Models as a new paradigm in AI, operate by starting with pure noise, employ a multi-step iterative process, then finally refine the data by removing the input noise until it achieves a coherent output -like an artist sculpting from a block of marble- with exceptionally fine-grained details [78]. Figure 5 presents basic forward and reverse diffusion states,

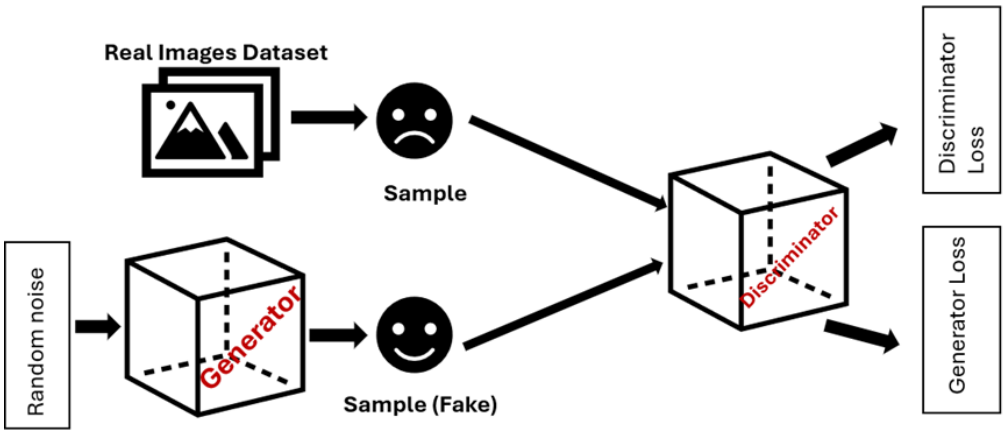


FIGURE 3. Basic working architecture of a GAN

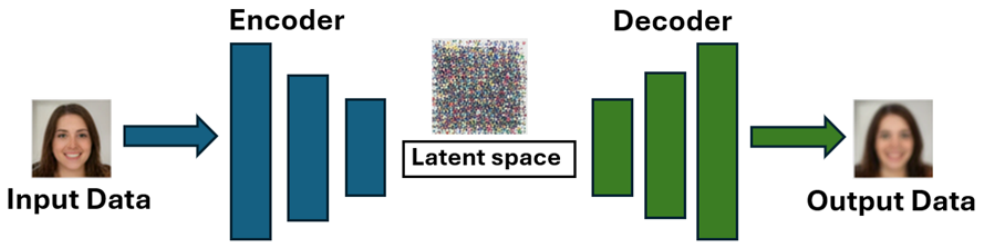


FIGURE 4. Basic working architecture of a VAE

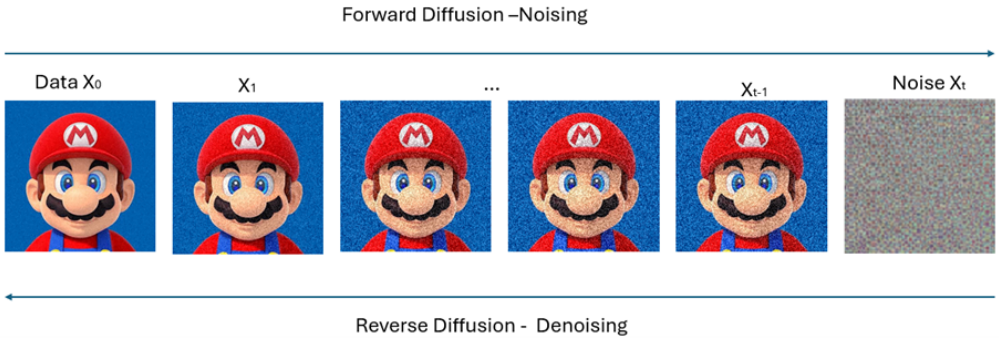


FIGURE 5. Basic forward and reverse diffusion states of a Diffusion Model

which took its principles from continuous-time stochastic processes. The forward diffusion process is modelled as a Stochastic Differential Equation (SDE), which systematically corrupts the data distribution into an easily sampled Gaussian noise [35].

While the older diffusion models struggled with the problem of audio-sync, modern models has achieved superior audiovisual consistency [50].

2.2. **Deepfake Techniques.** Aside from the generation algorithms, there are multiple techniques to create a Deepfake including “Face Swapping”, “Lip-syncing” and “Puppet”. Deepfake generation techniques for visual and video content

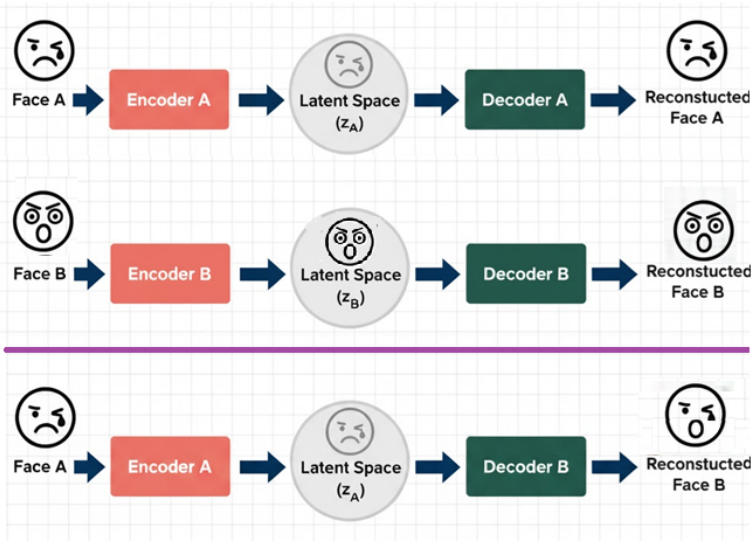


FIGURE 6. Face Swapping technique, training and construction phases

are notably diverse compared to other media types like *lip-syncing* methods, which align a person's lip-movements with an alternative audio track, and *face-swapping* techniques, which replace one person's face with another's [8].

Face Swapping aims to insert a face from a source- image or video- onto a target content. Training and generation processes of Face Swapping can be seen in Figure 6. Using AEs and GANs, the encoders transform the input data into latent code with critical features, which then transmitted to the decoder to reconstruct the original content based on the latent code. For this example, "Decoder B" can have any other input as latent face data to create similar faces to Face B [82].

Lip-syncing on the other hand, enables visual modification to be driven by audio modalities, to create a synchronization between lip movements and audio [85]. Neural network architectures -often built upon GANs or Diffusion Models- extracts relevant features from the input audio, such as phonemes or frequency coefficients, map these acoustic features to corresponding visual content including the lip shapes. A well-known example, Wav2Lip, uses an audio encoder and face encoder on the generator side and combines their output data to create lip-synced image, through face decoder. On the discriminator side, it uses the created lip-synced image and the original voice data through audio encoder and face encoder of discriminator to create multiple frames according to the synchronization [66].

Another approach is ***Puppet***, which facilitates the real-time or near real-time transfer of dynamic motion and expression from a *source* individual onto a *target* individual in a video. Puppet technique preserves the target's identity while altering its head and body movements and facial expressions, through the use of correspondence mapping, which establishes a pixel-level link between the source motion and the target face [53].

3. DEEPFAKE DETECTION

Various algorithms and approaches have also been developed for the ***detection*** of Deepfake content. According to a report published by the European Union Agency for Law Enforcement Cooperation (EUROPOL), Deepfake detection methods can be categorized into **automatic** and **manual** approaches. Automatic methods rely on the use of AI to detect and analyse Deepfakes -essentially employing AI to understand and counterattack AI- through algorithms specifically designed for this purpose. Manual approaches, on the other hand, are based on human perception and involve identifying anomalies or imperfections in less realistic content, which may vary depending on the type of media being examined [29]. Examples of such anomalies may include abrupt or unnatural transitions in facial expressions, irregularities in blinking patterns or frequency, artificial or monotonous vocal tones, inconsistent emphasis, unnatural speech pacing, mismatches between lip movements and speech, and violations of physical laws in environmental factors such as lighting and shadows [54].

Authentication methods include *metadata analysis* and *digital watermarking*. ***Metadata*** techniques involve embedding information about the content's creator, modification history, and timestamps with the file itself. Missing or altered metadata often signals manipulation; however, factors such as cross-platform sharing, device transfers, file compression or resizing can also result in metadata loss [34]. Content Credentials (CC) from Adobe are durable, industry-standard metadata type which acts like a digital nutrition label for content and include details about the creator and the creation type of the content as if it was captured by a camera or generated by AI [1]. Adobe not only develops its own solutions in the field of authenticity verification but also leads the way in establishing *global standards*. In this context, the Coalition for Content Provenance and Authenticity (C2PA), formed with the participation of various industry stakeholders, aims to make the provenance and authenticity of digital content traceable and verifiable based on technical standards. The technical rules published by C2PA in 2022 represent an important step towards implementing standards for content provenance information based on CC usage and developing technical improvements in line with these standards [14]. Similarly, the CAI (Content Authenticity Initiative), established by Adobe in 2019, aims to raise awareness, develop educational models, and make the verification of *content origin* scalable and accessible in the digital ecosystem to be created through the development of open-source tools based on the C2PA standard, with over 5,000 members from various sectors such as civil society, media, and technology [15]. ***Watermarking***, on the other hand, involves embedding a logo, signature, or text fragment -either perceptible or imperceptible to the human eye- within the content [2]. When a modification occurs, the watermark may disappear or become distorted serving as an indicator of tampering [5].

Another helpful approach is ***labelling***, which refers to process of embedding a perceptible indicator into synthetic media to help viewers recognize that the content has been artificially generated [63]. In this context, creators of synthetic media, including Deepfakes, are encouraged to attach a *clear label* in a manner that does not interrupt the viewer's experience. While some platforms expect content creators to provide synthetic content labels before sharing, it is not reasonable to expect users to voluntarily label their content as synthetic since Deepfakes are mostly produced by malicious actors for the purpose of deception. In a study involving over 1,000 participants, more than half of the participants stated that they did not want to interact with content labelled as having been generated by AI [52]. Therefore, rather than relying on user declarations, some platforms run content through their own internal verification mechanisms during the upload phase and automatically label content if manipulation is detected, without seeking user declarations [10].

4. Deepfake Use Areas

Deepfake content offers users a wide range of opportunities across diverse fields such as education, art, advertising, culture, accessibility, healthcare, and psychology. Despite the numerous opportunities offered by Deepfakes, due to its nature of providing hyper-realistic convincing content, presents itself as an unparalleled tool in various crime scenarios. As an increasingly accessible service, often offered for free or at a minimal cost, and enabling the easy production of realistic content without requiring any expertise, Deepfake production applications mean that anyone can be the perpetrator of a Deepfake attack, and anyone can be the victim [28].

4.1. **Beneficial Areas.**

In the field of **education**, Deepfake technology can be used to create engaging learning materials that increase students' focus and interest by incorporating the likeness of their favourite characters or celebrities into educational content [71].

In **healthcare** and **psychology**, a notable example involves the use of Deepfake content in therapeutic contexts. It has been suggested that Deepfake filtering capabilities could be utilized in therapy sessions for patients suffering from conditions such as post-traumatic stress disorder (PTSD), allowing them to confront the subjects or scenarios that caused their trauma in a controlled therapeutic setting [36].

In terms of **accessibility**, Deepfake technology, offers transformative potential for patients with paralysis- such as those affected by ALS. By training AI models on their own voice data, such individuals could regain the ability to communicate their thoughts in their natural voice, even after losing physical speech abilities [18].

As an example of **awareness-raising** initiatives, an informational video on malaria disease featuring former football player David Beckham was produced using lip syncing technique, allowing it to be presented in 9 different languages [77].

Within the **entertainment industry**, one of the most common domains of Deepfake application, the technology has been used to digitally recreate deceased actors for appearances in sequel movies [57]. In more casual instances, social

media users employ Deepfake tools to impersonate celebrities and share content as though they were the public figures themselves [31].

In the **art** sector, an exemplary case can be found at the Dali Museum, dedicated to the renowned artist Salvador Dali. The museum used Deepfake technology to create a lifelike digital replica of the artist allowing visitors to interact virtually with a synthetic version of Dali, thereby enhancing their overall museum experience [6].

In **advertising**, companies may use Deepfake technology to produce promotional materials featuring celebrities in advertisement campaigns, enabling brands to promote their products using the likeness and voice of the public figures without requiring their physical participation during the production process [71].

Beyond the above-mentioned applications, Deepfake technology also holds promise in terms of supporting **law enforcement** and **judicial process**. It can be used to generate realistic training an simulation scenarios, convert witness testimonies into audiovisual formats to aid in case analysis, and create synthetic identities for undercover operations or personnel anonymization -thereby enhancing the effectiveness and safety of investigative and judicial procedure [28].

4.2. **Misuse Areas.** Due to its highly convincing nature, Deepfakes can lead to **financial**, **psychological**, and **social** harm on **individual**, **institutional**, and **societal** levels through various means such as *fraud, extortion, defamation, identity theft, disinformation, and erosion of trust* in information which is called as "infocalypse" in some sources [72] [18]. In this context, within the scope of this study, the potential misuse-cases are discussed under the following categories:

- Cyberbullying,
- Blackmail, exposure, defamation
- Disinformation and the spread of misinformation,
- Non-consensual intimate content,
- Identity fraud/scams,
- Erosion of trust in information,
- Interference with law enforcement and judicial processes,
- Violations of copyright and personality rights.

One of the most common problems encountered through the use of Deepfake content is **cyberbullying** which can be simply defined as *bullying with the use of digital technologies* [84]. It is a type of cybercrime frequently seen among students, especially from elementary school age onwards. The dissemination of realistic but non-existent content produced by Deepfake technology in various environments makes it possible to carry out targeted attacks within the scope of technological capabilities. A notable example occurred in New Jersey, where a high school girl filed a complaint to school administration that her face had been used in synthetic sexually explicit videos created by her classmates. Investigation revealed that Deepfake sexual content had been produced and shared about more than thirty female students at the same high school [41].

Another issue frequently mentioned alongside Deepfake attacks is **disinformation** and **misinformation**. The concept of *disinformation* refers to false, inaccurate, or misleading information deliberately produced, presented, and disseminated with the intent to harm a person, social group, institution, or country, while *misinformation* is defined as the sharing of false or inaccurate information without the intent to deceive [62]. Disinformation is created and disseminated with the intent to deceive [29]. According to the phenomenon known as the "*Colavita visual dominance effect*" people tend to place greater trust in visual information than in other sensory inputs [47]. In this context, the realistic nature of Deepfake content offers an unparalleled opportunity to persuade the targeted audiences. In a 2023 survey on AI applications in the US, 85% of participants expressed concern about the spread of misleading Deepfake audio and video content [32]. Another study found that 70% of participants who listened to Deepfake audio stated that they did not trust themselves to determine whether the content was authentic or not [13].

The societal impact of disinformation attacks becomes particularly pronounced during election periods, when public perception can be easily swayed by fabricated media. For instance, during the Slovak presidential elections, a Deepfake audio recording of allegedly featuring one of the candidates circulated online just days before the vote, raising concerns that it may have influenced the election results [22]. In another disinformation attack involving the use of Deepfake content and its societal impacts, a Deepfake video was released during the Ukraine-Russia war, in which Ukrainian President Volodymr Zelensky allegedly told his soldiers to surrender [37].

It has been observed that crimes such as **blackmail**, **defamation**, and **exposure** can also be committed as *cyber-enabled crimes* through the use of Deepfake content. The categorization made by the European Parliament states

that attacks such as blackmail, sexual blackmail, intimidation, defamation, and undermining trust are examples that can have psychological consequences [28]. There can be a wide variety of scenarios in blackmail, defamation, and disclosure-based Deepfake attacks. For example, a person may be financially exploited through fabricated media depicting them in compromising situations or coerced into revealing private information under the threat of exposure.

In 2023, over 95,000 Deepfake videos were detected, 98% of which fell into the category of **non-consensual sexual content**, and almost all of these target women [33]. It is stated that non-consensual Deepfake sexual content, which specifically targets women and children and can cause not only psychological but also social harm, sometimes serves as a digital tool of violence that deepens gender inequalities [59]. In one of the most widely known examples, the dissemination of explicit Deepfake content depicting the famous artist Taylor Swift on social media just before an award ceremony where the artist was expected to receive an award is, according to some sources, a sexist attack. The explicit Deepfake content belonging to Swift was viewed 47 million times before being removed by the social media platform on which it was shared [70].

Due to its convincing nature, Deepfake technology is a convenient tool for **fraud** and **identity theft**, and numerous attacks on various scales have been reported. In one example, a French fan was scammed out of €830,000 under the pretext of "cancer treatment" by being led to believe in a fake relationship through Deepfake content featuring Brad Pitt [23]. One of the most well-known and corporate examples is the Hong Kong case, where a Hong Kong-based company was defrauded of $25 million after attackers used Deepfake filtering to pose as senior executives and participate in an online meeting [17].

Another problem that Deepfake content can cause socially is the **undermining of trust in information**. The increasing trend in the quality and quantity of Deepfake content is replacing individuals' trust in the content they encounter online with suspicion. The ability of Deepfake content to create false evidence or discredit original evidence, especially in judicial proceedings, may lead to an erosion of trust in information within society. In a case in point, despite the highly clear and explicit video evidence presented to the court, the lawyer of a person named "Guy Refitt," who was tried in January 2021 in connection with the US Capitol riot, attempted to defend his client by claiming that the content in question was fake [83].

Deepfake content occupy a legally ambiguous territory in terms of **copyright** and **personality rights**. Copyright is a legal term used to define the rights that creators have over their literary and artistic works, and the works covered by it are considered on a broad scale, including books, sculptures, computer programs, and databases [89]. While the issue of copyright for AI-generated content stays in a controversial area, there are also uncertainties regarding copyright for Deepfake content, as a subcategory of AI-generated content. Various issues have arisen from different viewpoints, such as concerns regarding the copyright of the data used to train algorithms, whether content generated by AI is subject to copyright and, if so, who should own it, and concerns regarding the copyright of a work of art included in content generated by AI, such as a song playing in the background of a synthetically generated video content [24]. Concerns regarding personal rights have also arisen, as Deepfake technology can be used to produce content depicting identifiable individuals. For example, a lawsuit was filed alleging that the voice of famous actress Scarlett Johansson was used without her consent for the voice assistant "Sky" developed by OpenAI [56].

5. Information Security, Cybersecurity and Deepfakes

The concept of **information security** can be summarized as "*all efforts aimed at protecting important or valuable information*" [69]. Information security processes aim to ensure the *confidentiality, integrity,* and *availability (accessibility)* of information and information systems. In this context, **integrity** means that information is not altered or destroyed and is complete, accurate, and comprehensive; **confidentiality** means that access to information is restricted to authorized individuals for the purpose of protecting personal privacy and private information; and **availability** means that the desired information can be accessed reliably by authorized users at the desired time [61].

The term **cybersecurity**, as defined by the International Telecommunication Union, means "*... collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's*

assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation, Confidentiality." [39].

Although the terms "Information Security" and "Cybersecurity," are often used interchangeably in the literature, both share the common goal of preventing unauthorized access and use of sensitive data. In contrast, information security is an umbrella term that encompasses all measures and practices aimed at protecting every type of information assets – not limited to digital systems and cyberspace [79]. Thus, while information security provides protection for information regardless of its environment or format, cybersecurity is concerned exclusively with the digital domain and the data stored therein [4].

From an information security perspective, Deepfake contents poses a great risk, particularly in terms of protecting the integrity of information [71]. Through techniques such as impersonation of natural persons and identity theft, unauthorized access to information can be achieved, and acquired data can be manipulated- especially via Deepfake attack conducted over communication networks. These practices represent some of the most common and fundamental Deepfake-related threats within the framework of information security [58].

According to INTERPOL's definition, cybercrimes are divided into two categories: "*cyber-enabled crime*" and "*cyber-dependent crime*". Cyber-enabled crime refers to traditional crimes supported by cyber capabilities, while cyber-dependent crime refers only to crimes that can be committed using computers, computer networks, and other information and communication technologies, targeting information and communication systems [21]. Since Deepfake production and manipulation occur in virtual environments, most attacks utilizing this content could be classified as **cyber-enabled attacks**. Common forms of Deepfake-enabled attacks include cyberbullying, extortion, exposure and defamation, disinformation and misinformation campaigns, production of non-consensual explicit material, identity fraud and impersonation, erosion of trust, interference with law enforcement and judicial processes, and violations of copyright and personality rights. Because the creation and dissemination of Deepfake content typically involve the digital manipulation and distribution of data, these activities inherently fall within the scope of cybersecurity concerns.

6. Regulatory Approaches on Deepfakes

Various countries have adopted different regulatory and strategic approaches to tackle misuse of Deepfake content. While some countries regulate Deepfake content under specific headings such as ***election security*** or the production of ***non-consensual sexual content***, many countries, including Türkiye, do not have any specific regulatory approach addressing Deepfake content. Examples of regulations addressing Deepfake content in general are quite limited. Given the cross-border nature of these attacks which involves the country of the origin, the jurisdictions where the content shared, the locations of both the victim and the perpetrator, and the regulations applicable to the platforms that host or distribute such content, the need for a uniform and harmonized international approach to effectively combat Deepfake-related threats increasing each day. Some of the notable examples on Deepfake regulatory approaches will be explained in the following sub-sections.

Law enforcement agencies are also making various recommendations against Deepfake attacks and are part of awareness and support mechanisms to ensure the sustainability of the processes. For example, the UK police force has established a website where Deepfake content can be reported, covering areas such as sexual blackmail and harassment, defamation, fraud, terrorist propaganda, hate crimes, and child abuse [55, 65] . Also, an FBI report emphasized that the use of generative AI technologies to produce image, audio, video, and text content has enabled a significant increase in fraud activities and outlined possible countermeasures. These measures include:

- Selecting a secret word or phrase as a password among family members, using this password as a verification mechanism in potential Deepfake attacks that could be carried on family members,
- Evaluating visual and audio content for various flaws such as inappropriate shadow placement and unrealistic movements to determine whether it is a Deepfake,
- Carefully evaluating the tone of voice and choice of words in phone calls claiming to be from loved ones to determine whether one is being subjected to a Deepfake attack,
- Limiting social media sharing as much as possible, making accounts private if possible, and filtering the number of followers to limit the supply of personal data necessary for training and production to attackers in the online environment [30].

6.1. **China.**

China has introduced strict rules on the **creation** and **distribution** of Deepfake content with the "Deep Synthesis Regulation," which came into effect in 2023. The definition of "Deep Synthesis" in the regulation refers to

the use of AI to create or modify digital information. Also, with the enforcement of new regulation on 1 September 2025, China's regulatory approach obligates artificially generated content to be clearly **labelled** and user identities to be verified [51]. Additionally, platforms must take technical measures to detect and remove such content. The actors included in the regulation are:

- "Synthetic Content Providers" refer to companies or platforms that **produce** or **share** AI-generated content and,
- "End Users" refer to individuals who **view** or **use** synthetic content [19].

One feature that distinguishes this regulation from other examples is the inclusion of technical obligations with detailed explanation. For example, while many regulations impose an obligation to label Deepfake content under transparency and information obligations, the Chinese regulatory approach highlights issues such as the requirement for such labelling to be visible to end users as well as at invisible metadata levels, how content labelling can be done according to different content types, the obligation to design content labelling processes to operate automatically, and to regularly test their functionality.

Responsibility for the implementation of the regulation has been assigned to the Cyberspace Administration of China. Under the regulation, users are expected to provide IDs or phone numbers to enable the establishment of application or platform registrations related to Deepfake production. Platforms are also expected to facilitate complaint mechanisms for victims of Deepfakes by establishing easy complaint channels [28].

6.2. **European Union.** European Union Artificial Intelligence Act (EU AI Act), which came into force in 2024, follows a risk-based approach that categorizes AI systems as "unacceptable risk," "high risk," "limited risk," and "minimal risk". The use of Deepfake technology falls under the ***limited risk*** category, creating an obligation of content subject to more limited transparency obligations to make sure that end users are expected to be aware that they are interacting with an artificial intelligence system [28].

Deepfakes defined in EU AI ACT as "... *AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.*". According to Recital 134 of the EU AI Act, deployers who use AI systems to **generate** or **manipulate** image, audio or video content that appreciably resembles real persons, objects, places, entities or events — and that would falsely appear authentic to a viewer are required to make a clear and distinguishable disclosure that the content has been artificially created or manipulated. Article 50(4) translates this principle into a binding obligation by explicitly requiring deployers of AI systems that produce or alter Deepfake image, audio or video content to disclose the synthetic origin of that content, subject to narrowly drawn exceptions (for example, law-authorised uses for detecting, preventing, investigating or prosecuting criminal offences) and a proportionate accommodation for artistic, satirical or analogous works so as not to impede their display or enjoyment. Finally, Article 99 foresees that in case of non-compliance, fines of up to EUR 15,000,000 or up to 3% of platforms total worldwide annual turnover shall be subjected [26].

Another regulatory approach from EU lies within Digital Services Act (DSA), although it does not contain a definition or reference to "Deepfakes," it provides a secondary regulatory framework for preventing the spread of malicious Deepfake content by imposing content moderation obligations on platforms. As stated in Recital 50 of DSA, in the event of the sharing of illegal or harmful content, platforms are obliged to remove such content after receiving a warning, excluding closed communication platforms like WhatsApp [87].

6.3. **South Korea.** South Korea has focused on two main themes in combating the threats posed by Deepfakes: **election security** and **privacy**. In terms of election security, the "Public Official Election Act" updated in late 2023, prohibits the production of Deepfake content related to candidates and political actors during the last 90 days before the election. Violation of the regulation may result in up to 7 years in prison or a fine up to 50 million Korean Won. Following the implementation of these changes, 129 violations were detected and removed from circulation during the 2024 elections in Korea [3] .

Another approach from South Korea aims to tackle non-consensual Deepfake imagery. A study found that 53% of the 95,820 Deepfake pornographic content identified in 2023 was produced in South Korea, indicating that South Korea ranks first globally in the production of non-consensual sexual Deepfakes. Also, same study underlined that, 8 of the top 10 individuals most frequently targeted by Deepfake pornography are South Korean female singers [73]. In this context, "Deepfake Sex Crime Prevention Act" has added new dimensions and penalties to the existing "Sexual Violence Prevention and Victims Protection Act" and the "Act on the Protection of Children and Youth against Sex

Offenses" [40]. Following the 2024 amendment, Deepfake pornographic content produced without the person's consent and approval is classified as a "digital sex crime," with penalties of up to five years in prison and fines imposed not only on those who **produce** or **share** such content but also on those who **view** or **store** it [76].

6.4. **United States of America.** There is a wide variety of Deepfake laws at the ***state*** level in the US. Among these, California's AB 730 law prohibits the **dissemination of manipulated content** intended to damage a **candidate's reputation** in the last 60 days before an election, but the regulation has raised various concerns regarding freedom of expression [16]. Regarding non-consensual sexual Deepfake content, California's AB 602 law grants a special right of action for placing a person's face in pornographic content without their consent. Similarly, the regulation introduced in New York State in 2020, grants artists a special right of action against such content, as well as a "right of posthumous recognition" mechanism, under which synthetic content depicting them can be challenged for 40 years after their death [49].

The Take It Down Act, passed at the ***federal*** level in US, in 2025, regulates the rapid removal of non-consensual intimate content, including Deepfakes, and criminal liability, with particularly severe penalties for images involving children [74]. The regulation stems from a Deepfake school incident that occurred in a Texas high school. After non-consensual Deepfake sexual content belonging to one of the students was spread on social media platforms such as Snapchat, it was found that Texas law had no provisions penalizing the use of Deepfake content. As the incident took place outside school grounds, the school was unable to impose any sanctions [12]. The regulation is grounded in the existing "Communications Decency Act", which governs the dissemination of private content, and the "Federal Trade Commission Act", which establishes the obligations imposed on online platforms. Penalties for violations include imprisonment, fines, or both, and differ depending on whether the offense involves adults or minors [20].

7. Deepfakes and Personal Data

Personal data, as defined by the Personal Data Protection Authority of Türkiye (KVKK), refers to *any information pertaining to identified or identifiable natural persons*. However, within the framework of the relevant regulation, such data may only be processed upon obtaining explicit consent, except in cases specified by law [43]. As a necessity brought by rapidly developing technology, regulations have been put in place in Türkiye, as in other countries, to ensure the protection of personal data, and the Personal Data Protection (Law No. 6698) has entered into force.

Biometric data refers to data that can be obtained effortlessly without any intervention and generally remains unchanged throughout a person's lifetime. Biometric data is listed among special categories of personal data in Article 6 of Law No. 6698, meaning that it may only be processed with explicit consent or in cases expressly permitted by law. According to the definition in Article 4 of the European Union General Data Protection Regulation (GDPR), biometric data is defined as personal data resulting from specific technical processing relating to the **physical**, **physiological**, or **behavioural** characteristics of a natural person that enable or confirm the unique identification of that natural person [27]. Physiological and physical biometric data includes information such as a person's fingerprint, facial features or vascular pattern, while behavioural biometric data includes distinctive movements reflected in a person's behaviour, such as walking style, typing style, pen grip angle and pressure, and driving style [44].

In terms of synthetic media produced with Deepfake technology, it is seen that personal data violations may occur in Deepfake content production when the subject is identifiable real persons. It can be considered that the security of behavioural biometric data is also violated, as the person's facial expressions and movements are imitated, in addition to physical biometric data such as the person's facial features. The status of personal data in Deepfake production targeting deceased individuals and the scope of consent in Deepfakes produced are other problems encountered. Furthermore, even in cases where consent is involved, there are concerns about ensuring the security of the processed data.

7.1. **Deepfakes and Personal Data Concerns.** One of the reasons why Deepfake technology poses a great threat is that the use of fake videos and audio, achieved through the manipulation of personal data has led to the increasing prevalence of potential threats such as manipulation, financial damage, cyberbullying, and fraud [54]. Even if none of the crimes mentioned in the previous section are committed using Deepfakes, the production and existence of Deepfake content can lead to personal data breaches.

The definition of Deepfake under the European Union Artificial Intelligence Act (EU AI ACT) is "... *AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.*". As stated in the definition, existing persons are among



FIGURE 7. An example of Deepfake that does not constitute a personal data breach in terms of output. (Produced with GeminiAI)

the subjects that Deepfake content can depict. Therefore, the processing of personal data is necessary to enable the production of Deepfake content related to real persons [25]. The manipulation of personal data such as voice and image using Deepfake technology results in a personal data that is far from reality, creating a hybrid content that is not real but contains real personal data [46].

Today, people share their personal information in digital environments and use this information to access various digital services [43]. These data can be used as input in the training processes of algorithms to enable the production of Deepfake content. The existence of **consent regarding the data used to train the Deepfake algorithm** constitutes the first of the Deepfake personal data concerns. In this context, algorithm providers and the parties intending to use such algorithms for content creation are required to obtain the explicit consent of the individuals whose personal data are used in the training datasets of the algorithm, in accordance with the *principle of transparency*.

Another personal data concern arising from Deepfakes relates to the **creation of content depicting identified or identifiable natural persons** engaging in actions they have never actually performed. Even if consent has been obtained for the use of personal data in algorithm training, producing Deepfake content that portrays identifiable persons without their explicit consent constitutes a personal data breach [28]. For instance, an attacker aiming to spread disinformation and undermine public trust in the army could produce and disseminate a Deepfake video depicting a soldier assaulting an elderly woman from an ethnic minority (Figure 7), thereby fabricating an event that never actually occurred. However, in this case, the Deepfake does not portray a real or identifiable soldier, nor an identifiable elderly woman. Therefore, the only potential concern regarding this content could be personal data infringement which relates to whether explicit consent was obtained for the personal data used in the algorithm's training process.

Another concern is the uncertainty of the **scope of the consent** obtained, both in terms of algorithm training and content creation. For instance, a well-known artist who consents to the creation of Deepfake content for a product's marketing campaign may face the risk that their personal data could later be used to generate outputs beyond the scope of their consent. If the artist cannot effectively limit how the trained algorithm or the resulting Deepfake content is used, the data initially provided for the advertising campaign may be repurposed for other production processes without authorization.

The use of Deepfake **content involving the personal data of deceased individuals**, either for generating synthetic media or as part of training datasets, constitutes another dimension of personal data concerns related to Deepfake technology. For instance, if a film star were to be posthumously featured in a new production by Deepfake algorithms

trained on their personal data, the critical question arises: *from whom and under what legal authority could explicit consent for the use of such personal data can be obtained?*

Even in the cases where explicit consent is duly obtained for the processing of personal data in Deepfake production, significant concerns remain regarding to the **protection of the consented datasets** used for either training or generation. Unauthorized access or misuse of these datasets by attackers could result in serious information security breaches and personal data violations. The safeguarding of training data- often containing sensitive biometric features- thus represents a crucial element in ensuring the lawful and ethical deployment of Deepfake technologies.

7.2. **Examples on Deepfake and Personal Data Breaches.** Any Deepfake production or algorithm training activities conducted without obtaining the person's consent for the processing of their data constitute a personal data violation. It is considered that the fact that the produced data is synthetic does not change the fact that the person in the data is recognizable, identifiable, and that the content can be associated with a natural person [67]. In this context, some examples of Deepfake attacks that are obvious due to the nature of the incident involving a personal data breach will be discussed in this section.

In such cases, the clearest evidence that consent for the use of personal data was not obtained for Deepfake training and content creation is when individuals only become aware of their inclusion in Deepfake content long after it has been produced and disseminated. In most cases, the target's biometric data is acquired without their knowledge or consent, either from their online activities, such as social media accounts, or, if the attacker is someone close to the individual, from photos, videos, and audio recordings captured by the attacker themselves. According to a study, politicians are the primary targets of Deepfake attacks, followed by celebrities, and the main reason for this is considered to be the easy access to training data [68]. In an example, a female victim who received a warning e-mail regarding sexual content being shared about her later discovered, upon investigation, that one of her closest friends had created Deepfake content using her images and disseminated it on the internet [86]. A study found that non-consensual sexual content production is most prevalent in South Korea, the US, and Japan, with 58% of the depicted individuals being singers and 32% being female actors. The same study, involving 1,522 male US citizens, reported that 74% of participants stated they did not feel guilty about watching non-consensual sexual content produced by Deepfake technology [73]. In this context, particularly in the production of Deepfake sexual content targeting famous women, it is assessed that personal data is not processed with consent, neither in terms of training algorithms nor content production.

The unauthorized processing of an individual's biometric data can also lead to **unauthorized access scenarios** to sensitive sources, such as bank accounts, mobile devices, and corporate systems containing confidential information. Research indicates that 42.5% of fraud cases today are AI-powered, and 29% of these attacks successfully succeed in breaching corporate security systems [75]. In a case study from 2024, despite the multi-layered security measures integrated into the system of a financial institution operating in Indonesia, attackers managed to bypass the identity verification processes in a Deepfake attack carried out through company's mobile application. The attackers, who are believed to have accessed the victim's identity information through various means, primarily social media and malware, managed to pass biometric verification by replacing the photo on the ID with Deepfake content. Although the method used varies depending on the structure of the identity verification processes, in this case, it is believed that Deepfake filtering applications were used to manipulate the identity photo to match the attacker and make the attacker's face appear like the victim's during the liveness test. The investigators also found that there were more than 1,100 Deepfake fraud attempts involving a single customer [38].

Another example of fraud involves the use of personal data obtained through social media posts to create Deepfake content, which is then used to defraud the Deepfake subject's relatives. These incidents often involve phone calls in which victims are led to believe that a loved one has been kidnapped or in distress and needs financial assistance [82]. A concrete example occurred in Florida in 2025, where a woman was defrauded of $15,000 after receiving a call claiming her daughter had been involved in a car accident that injured a pregnant woman and required legal assistance. The call featured Deepfake user attacker disguised as victim's daughter and another impersonating a lawyer [80]. A study reported that 6.5% of fraud cases examined in 2024 were supported by Deepfakes and that this rate has increased by 2137% in the last three years prior to the report [75].

Also, in terms of deceased persons, a relevant example can be found in the case of a commercial advertisement featuring the late actor Kemal Sunal, where Deepfake technology was applied to digitally recreate his likeness. According to the reports, it is stated that permission was obtained from the legal heir, the son of the late artist, in accordance with copyright procedures [42].

7.3. **Different Perspectives on Deepfake Personal Data Breaches.** Under Law No. 6698, in order to collect the training data required to produce Deepfake content, the **content creator** or **algorithm provider** must be the **data controller**. The data controller refers to the *natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data filing system*. Under Article 7 of Law No. 6698, the data controller is also responsible for **deleting** or **destroying** personal data ex officio or at the request of the data subject when the reasons for processing the data cease to exist. Under Article 10 of the aforementioned Law, the data controller is obliged to **inform** the data subject about the purposes for which the personal data will be processed. Under Article 11, the data subject has the right to;

- learn whether their personal data is being processed,
- request information about the processing of their personal data if it has been processed,
- learn the purpose of the processing of their personal data and whether it is being used for its intended purpose,
- request the correction of their personal data if it has been processed incompletely or incorrectly,
- request the deletion or destruction of their personal data in accordance with Article 7,
- seek compensation for damages resulting from unlawful processing [43].

From a GDPR perspective, the use of personal data for Deepfake training or production qualifies as "**processing**". GDPR protects **identified or identifiable natural persons** against potential personal data violations arising from Deepfakes, offering safeguards from multiple perspectives. Article 6 of the GDPR specifies six legal bases for processing, including;

- the data subject's consent
- the performance of a contract to which the data subject is a party or the taking of steps prior to entering into a contract,
- the processing is necessary for compliance with a legal obligation to which the data subject is subject or for the performance of a task carried out in the public interest,
- the processing is necessary for the legitimate interests pursued by the data controller or a third party, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

While it is considered that the mentioned provisions can be evaluated in terms of the **scope and ambiguity of consent in the processing of personal data in Deepfake production**, it is necessary for individuals who consent to the use of their personal data for training Deepfake algorithms or generating Deepfake content should exercise utmost caution in clearly defining the scope of their consent.

Deepfake production through personal data processing can be addressed in line with the legal conditions mentioned above, namely "*obtaining explicit consent*" and "*legitimate interests*". Under the GDPR, legitimate interests constitute the most flexible basis for personal data processing and apply fundamentally when an organization uses personal data in a manner reasonably expected by the data subject. Legitimate interests can refer to many things here, such as the commercial interests of an organization or a third party, or broader societal benefits. The validity of this condition generally depends on:

- The processing being clearly beneficial, even though it is not legally required,
- The risk of the processing must pose a low risk of infringing the privacy of data subjects and,
- The data subject must reasonably expect their data to be used in such manner.

In this regard, when evaluating the production of Deepfakes through the processing of personal data belonging to celebrities and politicians, it is considered that approaches for the purposes of satire and parody within the scope of **freedom of expression** are generally not considered contrary to the regulation. However, in cases of Deepfake use to produce non-consensual sexual content or for disinformation campaigns and fraud, there can be no legitimate interest in the use of the personal data of the individuals mentioned. Where legitimate interest does not apply, the processing of personal data is subject to explicit consent. In addition to content production, explicit consent must be obtained from the data subject when personal data processed for training purposes.

Instances where personal data are collected from individuals' posts — including those shared on social media — to facilitate the creation of Deepfakes are frequently observed. Within the framework of Law No. 6698, it is stipulated that publicly available personal data may be processed only to the extent that it aligns with the individual's intention in making it public. Given that there is generally no explicit declaration of intent permitting the use of social media content for Deepfake production or algorithm training, processing such data without obtaining consent would constitute a violation of the law [45].

Although individuals do not hold **copyright** over their own images in the general approach, various regulatory approaches exist in countries such as France, Germany, and Spain to ensure the protection of a person's image or portrait [28]. In the case of Denmark, where Deepfake content is addressed in terms of personal data and personality rights, changes are being made to the existing copyright law, stating that *every individual has rights over their own body, facial features, and voice*, and that the production and sharing of realistic imitations generated by AI without consent is considered as a crime. Under the proposed regulation, individuals whose Deepfake content is produced without their consent will be able to request the removal of such content, and platforms that fail to remove it will be subject to various sanctions [7]. Regarding copyright concerns, a report published by the World Intellectual Property Organization (WIPO) states that the creator of Deepfake content is the individual or entity that technically develops the algorithm or employs the model. In this context, the person depicted in the Deepfake is considered an actor not directly involved in the creation process; therefore, provided that they have consented to the use of their personal data, the intellectual property rights to the Deepfake content should belong to its creator. According to WIPO's view, the person or persons depicted possess only limited rights of approval or objection, primarily within the scope of personality rights [88].

Concerning **deceased persons**, Recital 27 of the GDPR explicitly stipulates that its provisions do not apply to the personal data of deceased individuals, while allowing Member States to establish their own rules regarding such data. In this context, Denmark has proposed a regulation that would allow relatives of the deceased to file compensation claims in cases where synthetic media is produced within the scope of the rights held by their citizens for 50 years after their death [64]. In Türkiye, under Law No. 6698, the concept of personal data presupposes the existence of a **living natural person**. In line with Article 28 of the Turkish Civil Code No. 4721, personality begins at the very moment the child is full born and ends by death [81]. Consequently, the use of personal data belonging to deceased person occupies an ambiguous and legally sensitive space, as such data no longer fall within the scope of the Law No. 6698.

In cases where consent is obtained for the processing of personal data for Deepfake algorithm training or production, it is necessary to encrypt or anonymize consented datasets to ensure their security under GDPR Article 32, establish information security processes in the context of confidentiality, integrity, and availability, and take technical and organizational measures. In the event of a breach involving such data, the data controller is obliged to **notify** the relevant supervisory authority within 72 hours under Articles 33 and 34, and to notify the data subject if there is a risk. Similarly, Article 12 of Law No. 6698, which addresses data security obligations, regulates the unlawful processing of personal data, security measures regarding access and storage, accessibility for purposes other than processing, and the obligation to report violations to the KVKK.

8. Conclusion and Recommendations

This paper has provided comprehensive analysis of Deepfake technology, tracing its evolution from foundational Deep Learning algorithms like GANs, VAEs, and Diffusion Models to its current state as a powerful and accessible tool. We have established that Deepfakes represent a significant **dual-use** technology. While its beneficial applications in education, healthcare, arts, and accessibility are promising, the potential for malicious use poses a substantial and growing threat to individuals, institutions, and society at large.

A central finding of this study is the profound challenge Deepfakes pose to the core tenets of **information security**-particularly in terms of *integrity and confidentiality*- as well as to **cybersecurity** and **personal data protection**. The technology's reliance on processing vast amounts of personal, often biometric, data creates significant legal and ethical ambiguities. As analysed, the unauthorized collection and use of this data for training algorithms or generating content frequently violate data protection frameworks, especially concerning the complex issues of **explicit consent** and the **scope of consent, copyright, personality rights and the legal status of deceased individual's data**.

The daily improvement and increase in the quality and quantity of Deepfake content complicates the fight against Deepfake-based cybercrimes, including Deepfake-based personal data breaches. The *multidimensional* and *complex* nature of Deepfake technology necessitates a multidimensional and multidisciplinary approach to combating it. Anyone can be the subject of Deepfakes, and various measures must be taken regarding the protection personal data.

Various actors involved in the production and dissemination of Deepfake content have various responsibilities to prevent personal data breaches using Deepfake technology. In this regard, the primary responsibility of **individuals** can be expressed as *minimizing the sharing of personal data* in online environments, making social media accounts private if possible, and being selective about the quality and quantity of followers. There is a need to enhance *awareness*

and *education* efforts so that individuals can be more conscious in online environments and prevent the misuse of their personal data against various threats, especially the threat of Deepfake. As a result of these efforts, individuals will be able to approach the content they encounter in online environments, especially on social media, with a questioning and critical perspective, aware that it could be a Deepfake. It is also beneficial to focus awareness efforts on **children** and the **elderly**, who are seen as vulnerable in terms of protecting their personal data in the cyber environment.

Regulatory and supervisory authorities must clarify the chain of legal **responsibility** and regulate the responsibilities of *producers, distributors, platforms,* and *data providers*. This requires maintaining active oversight mechanisms, primarily through regular reporting and auditing. The use of Deepfake content to violate personal data may be subject to criminal and administrative sanctions under relevant regulations, thereby potentially deterring such offenses before they occur. In this context, it is also critically important that individuals who encounter personal data breaches are provided with rapid application and resolution mechanisms, primarily by **law enforcement** and **judicial authorities**. In particular, there is a need to design and implement follow-up processes to ensure that victims of Deepfake attacks involving personal data breaches can remedy the harm they have suffered online, primarily through their right to be forgotten.

In this context, there is a need for **responsible data processing policies and the ethical use of AI, primarily by actors that enable closed communication** (such as WhatsApp, Telegram, etc.), **social media platforms** (X, Facebook, Instagram, TikTok, etc.), and **algorithm providers** need to design and implement measures in their internal processes, to combat Deepfake personal data breaches. **Content creators** should **label** Deepfake content before dissemination so that viewers interacting with it can understand that they are interacting with a synthetic media. The platforms should scan content prior to upload, using detection and verification algorithms and provide labelling for content assessed as Deepfakes. Algorithm providers should ensure that the training data used is obtained with explicit consent and used within the scope of it and integrate *authentication* processes such as *metadata* and *watermarking* into their algorithms. In the processes of collecting, storing, and processing data sets for Deepfake production or algorithm training, algorithm providers and content creators must jointly maintain their processes with *transparency* regarding personal data breaches.

Future research on Deepfakes and personal data protection should adopt a *multidisciplinary perspective* that integrates **technical** innovation, **legal** regulation, and social awareness. On the technical side, studies can focus on developing more robust and explainable detection algorithms that can adapt to rapidly evolving generation methods. In parallel, further work is needed on secure data governance mechanisms, particularly privacy-preserving model training methods to minimize the risk of personal data leakage during model training processes. Also, future research can analyse the adequacy of existing data protection framework in addressing synthetic media challenges. Comparative studies could explore the harmonization of national and international regulations concerning consent, liability, and the post-mortem use of personal likeness.

Declaration of Ethical Standards

The authors of this paper declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Authors Contribution Statement

Both authors participated in writing, reviewing, and approving the final manuscript.

References

[1] Adobe, 'Watermarking Photography: How to Protect Your Photos — Adobe', Adobe. Accessed: Sept. 12, 2025. [Online]. Available: https://www.adobe.com/uk/creativecloud/photography/discover/watermarking-photography.html.

[2] Adobe, 'Content Credentials overview', Content Credentials'a genel bakış. Accessed: Nov. 02, 2025. [Online]. Available: https://helpx.adobe.com/content/help/tr/tr/creative-cloud/apps/adobe-content-authenticity/content-credentials/overview.html.

[3] AI Incident Database, 'Incident 673: Deepfakes Circulating and Eroding Electoral Integrity in the Lead-up to 2024 South Korean legislative election' Accessed: Nov. 05, 2025. [Online]. Available: https://incidentdatabase.ai/cite/673/.

[4] Alexei, A., Alexei, A., *The Difference Between Cyber Security vs Information Security*, JES, vol. 29, no. 4, pp. 72–83, Dec. 2022, doi: 10.52326/jes.utm.2022.29(4).08.

[5] Anand, A., Singh, A.K.,*Watermarking techniques for medical data authentication: a survey*, Multimedia Tools and Applications, 20(2021), 30165–30197. doi: 10.1007/s11042-020-08801-0.

[6] Aouf, R.S., 'Museum creates deepfake Salvador Dalí to greet visitors', Dezeen. Accessed: May 20, 2025. [Online]. Available: https://www.dezeen.com/2019/05/24/salvador-dali-deepfake-dali-musuem-florida/.

[7] Axelsson, S., 'Owning the Self: Denmark's Copyright Turn Against Deepfakes', Schjødt. Accessed: Oct. 10, 2025. [Online]. Available: https://schjodt.com/news/owning-the-self-denmarks-copyright-turn-against-deepfakes.

[8] Ayata, O., 'Artificial Realities: Mitigations against Deepfakes', Digital Policy Hub, Waterloo, ON, Canada, Working Paper, 2024. [Online]. Available: https://www.cigionline.org/static/documents/DPH-paper-Ayata.pdf .

[9] Bergmann, D., Stryker, C., 'What is a Variational Autoencoder?', IBM. Accessed: Nov. 08, 2025. [Online]. Available: https://www.ibm.com/think/topics/variational-autoencoder .

[10] Bickert, M., 'Our Approach to Labeling AI-Generated Content and Manipulated Media', Meta. Accessed: Nov. 08, 2025. [Online]. Available: https://about.fb.com/news/2024/04/metas-approach-to-labeling-ai-generated-content-and-manipulated-media/ .

[11] Birrer, A., Just, N., *What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape*, New Media & Society, 27(2024), 6819-6838. doi: 10.1177/14614448241253138.

[12] Boyer, A., 'North Texas mom shares "deepfake" horror story as lawmakers look to close loophole — FOX 4 Dallas-Fort Worth', FOX 4 News. Accessed: Oct. 28, 2025. [Online]. Available: https://www.fox4news.com/news/deep-fakes-texas-artificial-intelligence.

[13] Bunn, A., 'Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam — McAfee Blog', McAfee. Accessed: Jun. 8, 2025. [Online]. Available: https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/.

[14] C2PA, 'C2PA Specifications'. Accessed: Sep. 4, 2025. [Online]. Available: https://spec.c2pa.org/specifications/specifications/2.2/index.html .

[15] CAI, 'Our members', Content Authenticity Initiative. Accessed: Sep. 12, 2025. [Online]. Available: https://contentauthenticity.org/our-members.

[16] California State Legislature, AB-730 Elections: deceptive audio or visual media, vol. AB-730. 2019. Accessed: Sep. 12, 2025. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730 .

[17] Chen, H., Magramo, K., 'Finance worker pays out $25 million after video call with deepfake "chief financial officer" — CNN', CNN World. Accessed: May 20, 2025. [Online]. Available: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html .

[18] Chesney, R., Citron, D. K., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, *SSRN Journal*, 2018, doi: 10.2139/ssrn.3213954.

[19] Choi & Partners, 'China Deep Synthesis Regulation 2025: Essential Guide', Choi & Partners. Accessed: Aug. 03, 2025. [Online]. Available: https://www.chinalegalexperts.com/news/china-deep-synthesis-regulation.

[20] Congressional Research Service, 'The TAKE IT DOWN Act: A Federal Law Prohibiting the Nonconsensual Publication of Intimate Images'. Accessed: Jun. 19, 2025. [Online]. Available: https://www.congress.gov/crs-product/LSB11314.

[21] Cross, S., Hirrle, S., Lim, M. A., 'Cybercrime Strategy Guidebook', INTERPOL, 2021. Accessed: Aug. 06, 2025. [Online]. Available: https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf .

[22] De Nadal, L., Jančárik, P., 'Beyond the deepfake hype: AI, democracy, and "the Slovak case", HKS Misinformation Review. Accessed: Aug. 06, 2025. [Online]. Available: https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/?utm.

[23] Dhaliwal, J., 'Breaking Down the Brad Pitt Scam: How it Happened and What We Can Learn — McAfee Blog'. Accessed: Nov. 12, 2025. [Online]. Available:https://www.mcafee.com/blogs/internet-security/brad-pitt-romance-scam-explained-how-to-prevent-scams/.

[24] Dilmegani, C., 'Generative AI Copyright Concerns & 3 Best Practices', AI Multiple. Accessed: Nov. 12, 2025. [Online]. Available: https://research.aimultiple.com/generative-ai-copyright/.

[25] European Parliament, 'EU AI Act: first regulation on artificial intelligence', Topics — European Parliament. Accessed: Nov. 12, 2025. [Online]. Available: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[26] European Parliament, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). 2024. Accessed: Sept. 19, 2025. [Online]. Available: http://data.europa.eu/eli/reg/2024/1689/oj .

[27] European Parliament and Council, *General Data Protection Regulation (GDPR) – Legal Text*, vol. (EU) 2016/679. Accessed: Nov. 12, 2025. [Online]. Available: https://gdpr-info.eu/.

[28] European Parliament Directorate General for Parliamentary Research Services, Tackling deepfakes in European policy, Publications Office, 2021. Accessed: Nov. 12, 2025. [Online]. Available: https://data.europa.eu/doi/10.2861/325063 .

[29] EUROPOL, 'Facing reality?: law enforcement and the challenge of deepfakes: an observatory report from the Europol innovation lab', Publications Office, 2024. Accessed: Nov. 12, 2025. [Online]. Available: https://data.europa.eu/doi/10.2813/158794.

[30] Federal Bureau of Investigation (FBI), 'Internet Crime Complaint Center (IC3) — Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud'. Accessed: Oct. 12, 2025. [Online]. Available: https://www.ic3.gov/PSA/2024/PSA241203.
[31] Fisher, M., 'TikTok - deeptomcruise'. Accessed: Nov. 10, 2025. [Online]. Available: https://www.tiktok.com/@deeptomcruise .
[32] Goldstein, J. A., Lohn, A., 'Deepfakes, Elections, and Shrinking the Liar's Dividend', Brennan Center for Justice. Accessed: Sep. 12, 2025. [Online]. Available: https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend.
[33] Gotsis, T. 'Sexually explicit deepfakes and the criminal law in NSW', Parliament of New South Wales, RESEARCH PAPER 2025–02, Apr. 2025. Accessed: Sept. 20, 2025. [Online]. Available: https://www.parliament.nsw.gov.au/researchpapers/Documents/Sexually%20explicit%20deepfakes.pdf.
[34] Guinard, D., 'C2PA and Digital Watermarks: A Powerful Combination Protecting Content Creators and Consumers', Digimarc. Accessed: Aug. 25, 2025. [Online]. Available: https://www.digimarc.com/blog/c2pa-and-digital-watermarks-powerful-combination-protecting-content-creators-and-consumers.
[35] Guo, Z., Lang, J., Huang, S., Gao,Y., Ding,X., *A Comprehensive Review on Noise Control of Diffusion Model*, Feb. 10, 2025, arXiv: arXiv:2502.04669. doi: 10.48550/arXiv.2502.04669.
[36] Hoek, S., Metselaar, S., Ploem, C., Bak, M., *Promising for patients or deeply disturbing? The ethical and legal aspects of deepfake therapy*, J Med Ethics, vol. 51, no. 7, pp. 481–486, July 2025, doi: 10.1136/jme-2024-109985.
[37] Holroyd, M., Olorunselu, F., 'Deepfake Zelenskyy surrender video is the "first intentionally used" in Ukraine war — Euronews'. Accessed: Nov. 2, 2025. [Online]. Available: https://www.euronews.com/my-europe/2022/03/16/deepfake-zelenskyy-surrender-video-is-the-first-intentionally-used-in-ukraine-war.
[38] Huang, Y., 'Deepfake Fraud — Group-IB Blog', Group-IB Blog. Accessed: Nov. 02, 2025. [Online]. Available: https://www.group-ib.com/blog/deepfake-fraud/.
[39] ITU-T X.1205, 'Definition of cybersecurity', ITU. Accessed: Nov. 1, 2025. [Online]. Available: https://www.itu.int:443/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx .
[40] Jeon, G. J., 'Korean parliament set to vote on bills to toughen punishments for deepfake sex crimes this week'. Accessed: Nov. 2, 2025. [Online]. Available: https://english.hani.co.kr/arti/english_edition/e_national/1159519.html.
[41] Johnson, A., 'NJ high schooler calls for AI regulations after manipulated pornographic images shared online', 6abc Philadelphia. Accessed: Aug. 26, 2025. [Online]. Available: https://6abc.com/post/francesca-dorota-mani-ai-generated-pornographic-images-westfield-high-school-nj-legislation/14019614/.
[42] Karcı, H.D., *Reklamcılıkta Deepfake Ugulamasına Neil Postman'ın Beş Fikirli Perspektifiyle Yaklaşmak: Durum Çalışması*, International Social Mentality and Researcher Thinkers Journal, 68(2023), 2864–2886.
[43] Kişisel Verileri Koruma Kurumu (KVKK), '6698 Sayılı Kanunda Yer Alan Temel Kavramlar', *KVKK*, Ankara, 97, 2025. Accessed: Apr. 20, 2025. [Online]. Available: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/b414e1cf-bd67-43f1-a6f9-3bff081f92e7.pdf.
[44] Kişisel Verileri Koruma Kurumu (KVKK), 'Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber', *KVKK*, Ankara, 55, Mar. 2025. [Online]. Available: https://www.kvkk.gov.tr/Icerik/7047/Biyometrik-Verilerin-Islenmesinde-Dikkat-Edilmesi-Gereken-Hususlara-Iliskin-Rehber.
[45] Kişisel Verileri Koruma Kurumu (KVKK), 'Örneklerle Kişisel Verilerin Korunmasına İlişkin Rehber.', *KVKK*, Ankara, 52, Mar. 2025. Accessed: Oct. 31, 2025. [Online]. Available: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/b654ee4e-e329-49a6-9722-03561daac1aa.pdf.
[46] Kişisel Verileri Koruma Kurumu (KVKK), 'Deepfake Bilgi Notu', *KVKK*, Ankara, 75, Apr. 2025. Accessed: Oct. 31, 2025. [Online]. Available: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/015794c4-061b-4560-a0b2-e372ee536642.pdf?trk=public_post_comment-text.
[47] Koppen, C., Spence, C., *Seeing the light: Exploring the Colavita visual dominance effect*, Experimental Brain Research, 180(2007), 737–754. doi: 10.1007/s00221-007-0894-3.
[48] Kossale, Y., Airaj, M., Darouichi, A., *Mode Collapse in Generative Adversarial Networks: An Overview*, 2022 8th International Conference on Optimization and Applications (ICOA), Oct. 2022, 1–6. doi: 10.1109/ICOA55659.2022.9934291.
[49] Lalla, V., Mitrani, A., Harned, Z., 'Artificial Intelligence: Deepfakes in the Entertainment Industry'. Accessed: Aug. 07, 2025. [Online]. Available: https://www.wipo.int/en/web/wipo-magazine/article-details/?assetRef=42620&title=artificial-intelligence-deepfakes-in-the-entertainment-industry.
[50] Liu, J., Wang, J., Hou, S., Ren, M., Wu, H., He, Z., *Beyond Face Swapping: A Diffusion-Based Digital Human Benchmark for Multimodal Deepfake Detection*, arXiv preprint arXiv:2505.16512, 2025, doi:https://doi.org/10.48550/arXiv.2505.16512.
[51] MA, X., 'Deep Synthesis Not Deepfake: How AI Compliance Works in China', China Law Vision. Accessed: Nov. 10, 2025. [Online]. Available: https://www.chinalawvision.com/2025/02/digital-economy-ai/deep-synthesis-not-deepfake-how-ai-compliance-works-in-china/ .
[52] Martin, J., 'The AI Trust Gap: 82% Are Skeptical, Yet Only 8% Always Check Sources', Exploding Topics. Accessed: Sep. 14, 2025. [Online]. Available: https://explodingtopics.com/blog/ai-trust-gap-research.
[53] Masood, M., Nawaz, M., Malik, K., Javed, A., Irtaza, A., *Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward*, Appl Intell, 53(2023), 3974–4026.
[54] McAfee, 'The McAfee AI Election Toolkit', *McAfee*, San Jose, CA, The McAfee Safety Series, 2024.
[55] Metropolitan Police, 'Deepfakes: help and support'. Accessed: Aug. 12, 2025. [Online]. Available: https://www.met.police.uk/advice/advice-and-information/online-safety/online-safety/deepfakes-what-is-a-deepfake/deepfakes-help-and-support/ .

[56] Milmo, D. 'Scarlett Johansson's OpenAI clash is just the start of legal wrangles over artificial intelligence', The Guardian, Aug. 28, 2024. Accessed: Nov. 3, 2025. [Online]. Available: https://www.theguardian.com/technology/article/2024/may/27/scarlett-johansson-openai-legal-artificial-intelligence-chatgpt.

[57] MIT Center for Advanced Virtuality, 'Media Literacy - Part 2, pg6', Media Literacy in the Age of Deepfakes. Accessed: Aug. 28, 2025. [Online]. Available: https://deepfakes.virtuality.mit.edu/part2/pg6/.

[58] Muhly, F., Chizzonic, E., Leo, P., *AI-deepfake scams and the importance of a holistic communication security strategy*, Int. Cybersecur. Law Rev.,6(2025), 53–61. doi: 10.1365/s43439-025-00143-7.

[59] Narvali, A., Skorburg, J., Goldenberg, M.,'Cyberbullying girls with pornographic deepfakes is a form of misogyny', The Conversation. Accessed: Aug. 10, 2025. [Online]. Available: http://theconversation.com/cyberbullying-girls-with-pornographic-deepfakes-is-a-form-of-misogyny-217182.

[60] Negreiro, M., 'Children and deepfakes', *European Parliament Members' Research Service*, July 2025.

[61] Nieles, M., Dempsey,K. Pillitteri, V. Y., 'An introduction to information security', *National Institute of Standards and Technology (NIST)*, Gaithersburg, June 2017. doi: 10.6028/NIST.SP.800-12r1.

[62] OECD, 'Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity'. *OECD Publishing*, 2024. doi: 10.1787/d909ff7a-en.

[63] OFCOM, 'Deepfake Defences 2 - The Attribution Toolkit', 2025, Accessed: Sept. 02, 2025. [Online]. Available: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/deepfake-defences-2/deepfake-defences-2---the-attribution-toolkit.pdf?v=402066.

[64] Patishman, H., 'Deepfake Regulations: AI and Deepfake Laws of 2025'. Accessed: Oct. 07, 2025. [Online]. Available: https://regulaforensics.com/blog/deepfake-regulations/ .

[65] POLICE.UK, 'Deepfakes'. Accessed: Aug. 10, 2025. [Online]. Available: https://www.police.uk/advice/advice-and-information/online-safety/online-safety/deepfakes-what-is-a-deepfake/.

[66] Prajwal, K., Mukhopadhyay, R., Namboodiri, V., Jawahar, C., 'A Lip Sync Expert Is All You Need for Speech to Lip Generation In The Wild', *Proceedings of the 28th ACM International Conference on Multimedia*, Oct. 2020, pp. 484–492. doi: 10.1145/3394171.3413532.

[67] Privacy Company, 'Deepfakes and the GDPR — Privacy Company Blog'. Accessed: Oct. 30, 2025. [Online]. Available: https://www.privacycompany.eu/blog/deepfakes-and-the-gdpr.

[68] Resemble.AI, 'Q1 2025 Deepfake Incident Report: Mapping Deepfake Incidents', Resemble.AI., 2025. Accessed: Aug. 26, 2025. [Online]. Available: https://www.resemble.ai/wp-content/uploads/2025/04/ResembleAI-Q1-Deepfake-Threats.pdf .

[69] Sağıroğlu, Ş., Siber Güvenlik ve Savunma: Önem Tanımlar, Unsurlar ve Önlemler, Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Bilgi Güvenliği Derneği, Ankara, 2018.

[70] Saner, E., 'Inside the Taylor Swift deepfake scandal: "It's men telling a powerful woman to get back in her box"', The Guardian, Jan. 31, 2024. Accessed: May. 28, 2025. [Online]. Available: https://www.theguardian.com/technology/2024/jan/31/inside-the-taylor-swift-deepfake-scandal-its-men-telling-a-powerful-woman-to-get-back-in-her-box.

[71] Saudi Data & AI Authority, 'Deepfakes Guidelines', 2024. Accessed: May 31, 2025. [Online]. Available: https://istitlaa.ncc.gov.sa/en/transportation/ndmo/deepfakesguidelines/Documents/SDAIA_Deepfakes%20Guidelines.pdf .

[72] Schick, N., Deep Fakes and the Infocalypse: What You Urgently Need To Know, Hachette UK, 2020.

[73] Security Hero, 'State of Deepfakes 2023', 2023. Accessed: May 28, 2025. [Online]. Available: https://www.securityhero.io/state-of-deepfakes/assets/pdf/state-of-deepfake-infographic-2023.pdf.

[74] Senate Of The United States [R-T. Sen. Cruz, Text - S.146 - 119th Congress (2025-2026): Take It Down Act, vol. S.146. 2025. Accessed: Jun. 18, 2025. [Online]. Available: https://www.congress.gov/bill/119th-congress/senate-bill/146/text.

[75] Signicat, 'The Battle Against AI-driven Identity Fraud', 2024. Accessed: Oct. 10, 2025. [Online]. Available: https://resources.signicat.com/hubfs/The-Battle-Against-AI-driven-Identity-Fraud-2024-Signicat.pdf?hsLang=en.

[76] Smith G., Brake, J., 'South Korea confronts a deepfake crisis — East Asia Forum'. Accessed: Nov. 2, 2025. [Online]. Available: https://eastasiaforum.org/2024/11/19/south-korea-confronts-a-deepfake-crisis/ .

[77] Sodji, L., 'How we made David Beckham speak 9 languages — Synthesia'. Accessed: Aug. 30, 2025. [Online]. Available: https://www.synthesia.io/post/david-beckham.

[78] Sohl-Dickstein, J., Weiss, E. A., Maheswaranathan, N., Ganguli, S., *Deep Unsupervised Learning using Nonequilibrium Thermodynamics*, Sep. 28, 2015, arXiv: arXiv:1503.03585.

[79] Taherdoost, H., *Cybersecurity vs. Information Security*, Procedia Computer Science, 215(2022) 483–487. doi: 10.1016/j.procs.2022.12.050.

[80] TRUȚĂ, F., 'Florida Woman Loses $15K to AI Voice Scam Mimicking Daughter in Distress'. Accessed: Nov. 2, 2025. [Online]. Available: https://www.bitdefender.com/en-au/blog/hotforsecurity/florida-woman-loses-15k-to-ai-voice-scam-mimicking-daughter-in-distress .

[81] Turkish Civil Code. Code: 4721. (2001) T.R. Official Gazette, 8, 24607. http://www.resmigazete.gov.tr/eskiler/2001/12/20011208.htm#1.

[82] U.S. Department of Homeland Security, 'Increasing Threat Of Deepfake Identities', 2021. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf .

[83] U.S. Department of Justice Office of Public Affairs, 'Texas Man Sentenced to 87 Months in Prison for Actions Related to Capitol Breach'. Accessed: May. 29, 2025. [Online]. Available: https://www.justice.gov/archives/opa/pr/texas-man-sentenced-87-months-prison-actions-related-capitol-breach.

[84] UNICEF, 'Cyberbullying: What is it and how to stop it — UNICEF'. Accessed: Nov. 10, 2025. [Online]. Available: https://www.unicef.org/stories/how-to-stop-cyberbullying.

[85] Weifeng, L., She, T., Liu, J., Li, B., Yao, D., Liang, Z., Wang, R., *Lips Are Lying: Spotting the Temporal Inconsistency between Audio and Visual in Lip-Syncing DeepFakes*, Advances in Neural Information Processing Systems, 37(2024), 91131-91155.

[86] West, K., "'I was deepfaked by my best friend"', Apr. 02, 2024. Accessed: Aug. 2, 2025. [Online]. Available: https://www.bbc.com/news/uk-68673390 .
[87] Whisperly AI, 'Deepfake Regulation in 2025'. Accessed: Aug. 02, 2025. [Online]. Available: https://whisperly.ai/deepfake-regulation/.
[88] World Intellectual Property Organization (WIPO), 'WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI)', WIPO/IP/AI/2/GE/20/1, Dec. 2019. Accessed: Nov. 03, 2025. [Online]. Available: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ind_lacasa.pdf.
[89] World Intellectual Property Organization (WIPO), 'Copyright'. Accessed: Aug. 26, 2025. [Online]. Available:https://www.wipo.int/en/web/copyright.
[90] Zucconi, A., 'Understanding the Technology Behind DeepFakes -'. Accessed: May. 12, 2025. [Online]. Available: https://www.alanzucconi.com/2018/03/14/understanding-the-technology-behind-deepfakes/.