Seeking to define deepfakes from U.S. state laws

Abstract
In six years, the word deepfake has gone from a niche on Reddit to the main object of research for hundreds of researchers and to the front line of concern of many policymakers. However, this transition did not lead to a faithful definition because it is still an in-flux technology. There is one sector, however, that is incompatible with vague and equivocal concepts: legislative production. In this study, we analysed the definitions of deepfakes (or synthetic media) in the laws of five states in the United States and proposed the key concepts that characterise them: artificial intelligence, fake/false and the reference (specific or generic) to the media that can support these deepfakes.

Keywords
Deepfakes, artificial intelligence, disinformation, synthetic media.

1. Introduction
The first reference to deepfakes came just over a year after the 2016 American presidential election, which was marked by the phenomenon of fake news (Gunther et al., 2018; Lee, 2019). Many feared that the following 2020 presidential election would also be marked by misinformation, in particular by a combination of fake news and deepfakes, but that did not happen (Meneses, 2021).

The deepfake that probably had the most impact on these elections turned out to be the one in May of 2019 that involved Nacy Pelosi: the then U.S. Speaker of the House appeared intoxicated and to be slurring her words as if she were drunk (Stewart, 2019). The point is that it was not a deepfake because it did not use artificial intelligence; rather, it was a cheapfake (or, less commonly used, a shallowfake), a video edited with much less sophisticated means than deepfake technology (Pawelec, 2022). The coexistence of deepfakes and cheapfakes increases the difficulty of distinguishing the two, as argued by Paris & Donovan (2019).

The impact that this type of disinformation can have on political discourse and future elections (Appel & Prietzel, 2022) is not irrelevant since it is deliberately altered audiovisual content that is amplified via social media. As for Pelosi’s video, the fact that it was based on edited software or simply changes in audio pitch made it at the same time easier to do and easier to detect, which is similar to what happens today with fake news.

What this example reinforces is the need to understand the nature of each phenomenon, to define it as correctly as possible, “to assist in the development of a consistent and theoretically coherent definition of deepfakes” (Whittaker et al., 2023).
Here is one example: When one of the first federal attempts in the U.S. to criminalise deepfakes (The Malicious Deep Fake Prohibition Act, 2018) defined the object as “any audiovisual record created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual,” Delfino (2019) advised that a definition of this type, without any limitations or modifiers, casts too broad a net to cover a lengthy range of media, including legitimate, non-offensive content like computer-generated imagery in films. The inclusion of such an overly-broad exemption would allow nearly every deepfake as long as the intention is not to cause harm, as in the case of a parody or satire (Chidera, 2023).

This is the primary objective of this paper: “if we can’t agree on what a deepfake is and is not, it makes the subject difficult to talk about” wrote Vincent in 2018. Five years later, the subject remains current.

To try to achieve this, we chose to analyse the way various state laws in the United States have been defining this technology. In no other area like justice is the importance of a correct definition so dramatic: just think that someone can be condemned or acquitted by a single word or even a comma in the wrong place (Kreps, 2023).

The choice of this specific sample and not others is essentially due to the combination of two factors: firstly, the characteristics of the legal autonomy of states in the U.S. that allow them to legislate on almost anything they want; and secondly, possibly because of what happened in the 2016 presidential elections, several U.S. states were pioneers worldwide in creating laws to penalise the use of deepfakes, even contradicting the widespread idea that legislative production is slow and hardly follows the way society evolves (Poritz, 2023). Although there are others, such as Delfino (2023), for whom states have been slow to enact deepfake legislation.

In fact, no other country in the world, with the exception of China (Hine & Floridi, 2022), has drawn up specific laws to regulate the creation of content through the use of artificial intelligence. On the European Union side, it is known that after the European Parliament approved (on June 14, 2023) its version of the Artificial Intelligence Act, the other bodies – the European Commission and the Council – will reconcile a final version for publication of relevant regulations.

Not even the United States itself, at the federal level, has done so to date, quite possibly because that would raise issues related to freedom of expression (Feeney, 2022; Loomis, 2022) and subsequent appeals to the Supreme Court of the United States. An example of these difficulties are the various efforts made especially in the U.S. Senate, all of which were unsuccessful (Wodinsky, 2021).

Therefore, as defended by Langa (2021), “a handful of states serve as laboratories, combating different threats posed by deepfakes by creating individual rights of action or protecting against election interference, among other methods.”

Another highly relevant issue is whether over the last few decades, the courts have become accustomed to considering the video as an authentic representation of events. With deepfakes, it will become increasingly more important to scrutinise such content and verify whether it is real or somehow artificially manipulated or generated (Europol, 2022).

The main research objective of this paper will not be achieved without taking into account the existence of several difficulties, starting with the fact that it is a new technology (based on artificial intelligence or AI), in permanent evolution (Delfino, 2023; Tashman, 2021; Ussenova, 2023) and with immeasurable future implications (Feeney, 2021).

Whittaker et al. (2023) studied the concept of deepfakes based on an external bibliographic review and concluded that “there is not yet universal agreement on a definition of deepfakes.”

The same authors added that, “Defining an innovative phenomenon such as deepfakes is critical because it allows for consistent and logical approaches to theoretical development and
empirical understanding, helping to mitigate fragmentation of the literature” (Whittaker et al., 2023).

The problem, upstream, is not just in the consensus of what a deepfake is but in the use of the word itself since if it has a negative/malicious connotation (Adee, 2020), and for this reason, it is already a crime in some states of the U.S. or in China; however, there are also uses of this technology that could simplistically be considered positive, such as in medicine (Gain, 2022), education (Truong et al., 2023) and art (Murphy et al., 2023). Danry et al. (2022) chose to talk about the beneficial use of deepfakes.

Hence, there are those who prefer the expression synthetic media (or, in the simplest form, synthetic video), although it is not clear whether this option solves the problem of the negative public image associated with deepfakes (Kerner & Risse, 2020; Lamb, 2022).

At this stage, and only for methodological purposes, we follow the definition proposed by Ofcom (2023) in the document “Synthetic media (including deepfakes) in broadcast programming”: “Synthetic media is an umbrella term for video, image, text, or voice that has been generated in whole or in part by artificial intelligence algorithms.” Note how the British telecommunications regulator uses the two concepts (deepfake and synthetic media) interchangeably.

Despite being based on legal documents, this research intends to be based on the spectrum of communicative doctrine, in the sense that it intends to contribute to a definition that facilitates communication of the concept studied. This does not invalidate the fact that it may eventually have some relevance in the legal area if its objectives are achieved.”

In addition to trying to characterise the concept of deepfakes (#Q1), this paper seeks to answer questions such as: ‘Has the concept evolved over time?’ (#Q2) and ‘What are the decisive elements upon which to build the concept?’ (#Q3).

2. Methods

A two-step diachronic methodology was used. First, a longitudinal bibliographic investigation was undertaken, which offered a systemic and detailed description including the most important features of the phenomenon. The bibliography was found through a Google Scholar search using the keywords “deepfake” and “deep fake” and their corresponding plural forms as well as “synthetic media.” This allowed us to complete a multidisciplinary systematic literature review to synthesise existing definitions of deepfakes. Second, we conducted an empirical analysis based on a research design of longitudinal studies of all the existing U.S. state laws that fit our methodology to identify the phenomenon and guarantee the validity of the results. Quantitative methods were used to identify deepfake definitions. To ensure interpretive accuracy, illustrative examples and quotations were matched to the emergent themes.

2.1. Explanatory notes

To build the research sample, it was necessary to create some rules:

- The laws to be analysed must explicitly refer to the words deepfake (or its variations of deep fake or deep-fakes, used interchangeably by authors such as Chesney and Citron [2019], or synthetic [media/video]). This question is quite relevant since in at least two cases, there was enormous confusion, not only among journalists but also among the academic community (Loomis, 2022; Nnamdi et al., 2023; Tashman, 2021; Vasquez, 2021): both the laws in force in Virginia (HB 2678, 2019) and in California (AB 602 and AB 730, 2019) are commonly referred to anti-deepfake laws, but the word is never used. As this is not a juridic investigation nor is its author a jurist who can make a legitimate hermeneutic of the texts in question, we understand that if the legislature chose not to make a direct reference, it is also not correct to do so in this context. In addition to Virginia and California, laws enacted in the states of New York (SB 5959, 2020), New Jersey (AB 4985, 2020), Georgia (SB 78, 2021), Wyoming (HB 0085, 2021) and South Dakota (22–21–4, 2023) also do not mention either of the two keywords. For example, the law passed in...
Wyoming (HB 0085, 2021) includes a “computer generated image that purports to represent an identifiable person.” An image created by Photoshop is a computer-generated image, but despite its impact, to the point of becoming an adjective, rare were the countries that created laws to regulate Photoshop. France was an exception and restricted it to any models appearing in commercial photography (Airey, 2017).

- Must be laws approved by the respective governor and to be in force. Two reasons may contribute to the exclusion in light of this assumption: either the bills were not approved in State instances (Illinois, Florida or Maine are good examples); or they were not in time to be considered for the sample of this investigation, which was concluded on 31 August 2023.

- There are several motivations for the legislature to criminalise the creation of deepfakes or, in certain cases, the dissemination of deepfakes, with the fight against non-consensual pornography (Chidera, 2023) or interference in election periods being the most notorious. But those are not the only motivations (Ferraro, 2019; Vasquez, 2021; Meskys et al., 2020). For our purpose, motivations are not relevant. Currently, no states completely ban the creation or distribution of all deepfakes.

- In this context, the type of liability, whether criminal or civil, imposed by the laws is also irrelevant (Coyer, 2023).

- This research also does not explore the technological aspect, namely what kind of artificial intelligence tools are used (machine learning, deep learning, generative adversarial networks, artificial neural networks, etc.), which could limit oneself to accepting this reality (see Vasquez, 2021 or Adee, 2020). Likewise, the different types of techniques used to develop deepfakes are irrelevant, the most common of which are face swap, lip syncing or the puppet technique (Department of Homeland Security, 2022).

Despite this being a recent technology, with the first research work on deepfakes only appearing in 2019, there is already substantial scientific production on the most varied aspects of deepfakes, above all, technical issues related to detection or their impacts (namely on women who are victims of this content). There is also extensive literature on the legal fight against deepfakes, as this paper demonstrates, but we believe that the approach proposed here is innovative.

To answer the three research questions, we divided this article as follows. First, we begin with questions related to the definition of deepfakes, concluding with a proposal.

We then move on to analyse the various state laws that meet the requirements that were established, looking for commonalities and fundamental differences.

Finally, we compared our proposed definition with the conceptualisation of deepfakes in the laws, answering the research questions.

3. Literature review: looking for a definition

A dictionary is the resource typically used by someone who needs to know the meaning of a word.

We started by putting together nine online dictionaries in which the word deepfake appears, plus Wikipedia (as there was no way to establish a sample with criteria, we opted for diversifying the sources).
Table 1. Definitions from online dictionaries.

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merriam-Webster¹</td>
<td>A deepfake is an image, or a video or audio recording that has been edited using an algorithm to replace the person in the original with someone else (especially a public figure) in a way that makes it look authentic. The fake in deepfake is transparent: deepfakes are not real. The deep is less self-explanatory: this half of the term is specifically influenced by deep learning—that is, machine learning using artificial neural networks with multiple layers of algorithms.</td>
</tr>
<tr>
<td>Macquarie²</td>
<td>A video of a computer-generated likeness of an individual, created using deep learning without the individual’s knowledge, often for the purpose of misinformation, vindictiveness, or satire.</td>
</tr>
<tr>
<td>Collins³</td>
<td>Deepfake is a way of adding a digital image or video over another image or video, so that it appears to be part of the original. A deepfake is an image or video that has been changed in this way.</td>
</tr>
<tr>
<td>Dictionary.com⁴</td>
<td>A fake, digitally manipulated video or audio file produced by using deep learning, an advanced type of machine learning, and typically featuring a person’s likeness and voice in a situation that did not actually occur.</td>
</tr>
<tr>
<td>Wiktionary⁵</td>
<td>A convincingly realistic but fake image, video, or audio created with the use of artificial intelligence, especially one that imposes the face of one person onto the body of someone else.</td>
</tr>
<tr>
<td>UrbanDictionary⁶</td>
<td>Deepfake is an advanced technique for human image synthesis based on artificial intelligence.</td>
</tr>
<tr>
<td>Oxford⁷</td>
<td>A video of a person in which their appearance has been digitally altered so that they look like somebody else.</td>
</tr>
<tr>
<td>Cambridge⁸</td>
<td>A video or sound recording that replaces someone’s face or voice with that of someone else, in a way that appears real.</td>
</tr>
<tr>
<td>Google D⁹</td>
<td>A video of a person in which their face or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information.</td>
</tr>
<tr>
<td>Wikipedia¹⁰</td>
<td>Synthetic media […] have been digitally manipulated to replace one person’s likeness convincingly with that of another. Deepfakes are the manipulation of facial appearance through deep generative methods.</td>
</tr>
</tbody>
</table>

Source: Own elaboration.

The first conclusion to draw is that the word ‘video’ (eight times) is predominant. That is, the overwhelming majority of dictionaries directly relate deepfake with video. There are also three references to ‘image,’ which reinforces the visual component of the concept. The word ‘audio’ appears in four queries and the word ‘text’ in none.

The two dictionaries that do not refer to ‘video’ or any other medium have the word ‘synthetic’ or ‘synthesis’ in common.

Another major element is ‘artificial intelligence.’ The expression can either appear explicitly (two times) or through derived techniques, such as ‘deep learning’ (three times) or ‘deep generative methods’ (once).

The four options that do not refer to artificial intelligence opt for the word ‘digital’ or ‘digitally.’

The approach to the word ‘fake’ is relevant since it belongs to the constitutive core of the concept.

Only three of the consulted sources used the word explicitly, which is added to ‘false’ (once) or ‘manipulated’ (once) or even ‘misinformation’ (once). In these last two cases, the association is only made by deduction, although it is obvious. In almost half of the consultations, the reader is either not informed about this feature or at least will have doubts.

(Only one of the dictionaries includes motivation as an element of the definition – ‘maliciously or to spread false information’ – although four refer to the aim of ‘appearing real’).

From the analysis of the keywords that the query allows (=Q3), it is possible to formulate a definition: deepfake is false/fake content created by AI (deep learning) through supports such as video, image or audio.

The main problem with this proposal is that it does not include the text as support.

3.1. The importance of the text

When the Reddit user first referred to videos of non-consensual pornography, he called himself ‘deepfakes.’ It is easy to understand that in 2017, deep (learning) + fake + video was the conceptual trilogy. What most of the consulted dictionaries have done is perpetuate this idea.

The first substantial alteration is the introduction of audio as an autonomous element, since in deepfake pornography videos, the overlay of the corresponding audio is not the most relevant element.

Interestingly enough, one of the first studies on the construction of deepfakes, although this exact concept was not used, was published in July 2017 and showed then-President Barack Obama speaking with accurate lip sync composited into a target video clip (Suwajanakorn, 2017).

During the following years, several authors only considered video as support for the fake content created by AI (Lussier, 2022; Maras & Alexandrou, 2019; Ternovski, 2022; Westerlund, 2019). On the contrary, Chesney and Citron in 2019 already referred to “hyper-realistic digital falsification of images, video, and audio.”

Although there are still those in 2023 who limit deepfakes to videos (Busaca & Monaca, 2023), more and more authors are considering audio (Europol, 2022; Whitaker et al., 2023; Somogyi, 2023).

In 2020, a Reuters investigation found that the author of half a dozen freelance editorials and blog posts with bylines in the Jerusalem Post and the Times of Israel did not exist. Basically, everything about “British student and freelance writer Oliver Taylor” was “an elaborate fiction” (Satter, 2020).

Although Reuters did not discover who was behind Taylor, today it would be possible to open up the authorship of the texts to VhatGTP or another AI-powered language model (Schwartz, 2023).

And if today the world has woken up to the reality of AI-generated text, there were those who realised at the time of its appearance that we were facing “the scariest deepfake of all"
(Diresta, 2020). To give more credibility to this resource, Meta presented in 2021 an AI research project called TextStyleBrush, which can copy the style of text in a photo using just a single word, promised Meta/Facebook (2021).

3.2. Proposing a definition

It is no longer possible to ignore the text element of any definition of deepfakes that may be presented, especially because in 2021, the European Parliamentary Research Service published a document stating that “Deepfakes can best be understood as a subset of a broader category of AI-generated ‘synthetic media,’ which not only includes video and audio, but also photos and text” (European Parliamentary Research Service, 2021).

The following year, the United States Department of Homeland Security released a document that reads: “Deepfakes, an emergent type of threat falling under the greater and more pervasive umbrella of synthetic media, use a form of artificial intelligence/machine learning (AI/ML) to create believable, realistic videos, pictures, audio, and text of events which never happened” (Department of Homeland Security, 2022).

The proposal by the British telecommunications regulator that we subscribed to at the beginning raises the same concerns: “‘Synthetic media’ is an umbrella term for video, image, text, or voice that has been generated in whole or in part by artificial intelligence algorithms” (Ofcom, 2023). In this definition, the ‘fake’ element is not directly valued, but it is deduced from the moment in which the content “has been generated in whole or in part by artificial intelligence algorithms.”

The definition proposed in the law that China put into effect at the beginning of 2023 goes in the same direction.

In the English translation, the expression ‘deep synthesis’ appears as a synonym for deepfake and the terms used are as follows: “Deep synthesis technology refers to the use of technologies such as deep learning and virtual reality, that use generative sequencing algorithms to create text, images, audio, video, virtual scenes, or other information” (China Law Translate, 2022).

As the most complete and restrictive law known, since it even includes music generation or 3D reconstruction, it describes among many other possible uses, “technologies for generating or editing text content, such as chapter generation, text style conversion, and question-and-answer dialogues” (China Law Translate, 2022).

At this point, it is already possible to state that the concept of deepfakes has evolved over time (#Q2). It went from only video to video and sound; word image was then added to video (which can be both synonymous with video or refer to photos); and only recently, did text begin to be considered.

It seems clear to us that any conceptualisation that may be made at this point must include: i) a generic or detailed reference to AI; ii) the idea of manipulated or fake content; and iii) the four supports or, alternatively, a generic and comprehensive formulation.

Fake/manipulated content in video, image, sound or text generated by AI?

There is, however, one element that cannot be ignored: the last three definitions use the word synthetic or synthesis.

Could it all boil down to synthetic media?

It is impossible to have an answer, but at least for the foreseeable future, the expression has to be accompanied by an explanation. What is synthetic media? It is fake/manipulated content in video, image, sound or text generated by AI.

As explained in the opening chapter, we consider both the word deepfake and the expression synthetic media for the purposes of analysing state laws.
4. Results

There are countless references in the media, in legal articles and even academic research to the fact that Virginia was the first U.S. state to legislate on deepfakes (March of 2019).

It turns out that the law in force makes no reference to either the word deepfake or synthetic (media), limiting itself to this: “creating, adapting, or modifying a videographic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person’s face, likeness, or other distinguishing characteristic” (HB 2678).

More notorious is the situation in California, which simultaneously passed two laws in 2019 (AB 602, aimed at victims of deepfake porn, and AB 730, in the context of an election campaign) that were immediately dubbed anti-deepfake laws.

Once again, neither law has any reference to the word (and the concept) deepfake, limiting themselves to describing “an image or an audio or video recording of a candidate’s appearance, speech, or conduct that has been intentionally manipulated in a manner such that both of the following conditions are met,” and explaining that “The image or audio or video recording would falsely appear to a reasonable person to be authentic” (AB 730).

Images created by photoshop or videos using stunts or special effects fit this description, which led Tashman (2021) to describe it as “a fairly holistic definition of what a deepfake is.”

In this way, the first law that meets the requirements set out in the methodology of this investigation (being a state law in force and referring to the words deepfake or synthetic) is the one that was approved in September 2019 in Texas.

According to these criteria, five laws will be analysed in detail in this chapter by chronological order of approval.

We have not included the law that was approved in Florida in 2022 (SB 1798) because doubts remain since the text of the law does not explicitly mention any of the keywords, although the official summary is unequivocal when it states that “Deep fakes are realistic images or videos that are created using artificial intelligence (AI) and often depict a real person saying something they did not say, or engaging in a behavior they did not engage in” (Bill analysis, 2022).

Several other laws were excluded for the same reason: They do not mention any of the two keywords. In addition to Virginia and California, there are laws enacted in the states of New York (SB 5959, 2020), New Jersey (AB 4985, 2020), Georgia (SB 78, 2021) and Wyoming (HB0085, 2021) that fit this criterion. Also, laws passed in South Dakota (22-21-4, 2023) and Illinois (HB 2123) avoid association with the key research terms, despite being passed in 2023.

In many other cases, bills were presented that, for various reasons and at different stages of the legislative process, were never enacted. The overwhelming majority did not even make it to the governors’ offices.

Finally, there were –until the moment when the field work for this investigation ended– several bills that followed the various stages of the legislative procedure and that may or may not have become laws.

A special note for New York, where it is possible to identify half a dozen attempts that for a variety of reasons either did not reach a successful conclusion or are still awaiting approval (Griner & Isaacson, 2023).

4.1. Texas (2019)

On September 1, 2019, Texas became the first state to prohibit the creation and distribution of “deepfake videos” intended to harm candidates for public office or influence elections (Ferraro et al., 2020).

The Texas law (SB 751), titled “Relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election,” defines a “deep fake video” as a video “created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality.”
Note the following about this law:
- It expressly limits deepfakes to video, which is understandable because it was published in 2019 but is also unfortunate because the failure to cover other means (whether naming them or in a generic formulation) makes it almost outdated at this time.
- The name of the law does not refer to deepfakes.
- There is no reference to AI.
- The idea of fake is described (indirectly) in this way: “[…] created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality.”
- This law is an important contribution to understanding how the concept has evolved over time (Q2).

4.2. Hawaii (2021)

It took almost two years before a new law emerged that explicitly invoked deepfakes as a crime, in this case, non-consensual deepfake pornography (Ferraro, 2021).

On June 23, 2021, law SB 309 became effective in the state of Hawaii, defining that “Deepfake technology enables the creation of synthetic media in which a person in an existing image or video is replaced with the likeness of another person.”

Note the following about this law:
- It starts to expressly contemplate the image in addition to the video (Q2).
- The concept of synthetic media appears for the first time.
- The word ‘deepfake’ (in this case, ‘deep fake’) appears in the name of the law (“Privacy in the first degree; deep fakes”).
- There is no reference to AI.
- The law indirectly explains the idea of false content: “a person in an existing image or video is replaced with the likeness of another person.”

A final note: This law follows the recommendations of a task force created in 2019 and designated the “Twenty-first Century Privacy Law Task Force.” An express request to the task force was that “Hawaii should protect the privacy of a person’s likeness by adopting laws prohibiting the unauthorized use of deep fake technology.”

4.3. Washington (2023)

On July 23, 2023, the State of Washington passed a law “Defining synthetic media in campaigns for elective office and providing relief for candidates and campaigns” (SB 5152).

“Synthetic media,” according to this legal text, “means an image, an audio recording, or a video recording of an individual’s appearance, speech, or conduct that has been intentionally manipulated with the use of generative adversarial network techniques or other digital technology in a manner to create a realistic but false image, audio, or video.”

Note the following about this law:
- The expression synthetic media reappears; however, the legislature chose not to make any reference to deepfakes.
- For the first time, there is a reference to audio in addition to video and image.
- For the first time, the AI is named (“generative adversarial network techniques”).
- Finally, for the first time, a law on deepfakes claims: “to create […] a false image, audio, or video.”

A final note: Since 2020, Washington legislators have been trying to pass a law with these objectives. In that year, a bill was presented in the Senate (SB 6513) that already spoke of “Deepfake audio or visual media.” In 2022, a proposal entitled “Restricting the use of synthetic media in campaigns for elective office” (SB 5817) was presented, which was also not approved. The law in force since 2023 is inspired by the latter.
4.4. Louisiana (2023)

On August 1, 2023, a law entered into force in the state of Louisiana that “Criminalizes deepfakes involving minors and defines the rights to digital image and likeness” (SB 175).

The law explains that “Deepfake’ means any audio or visual media in an electronic format, including any motion picture film or video recording, that is created, altered, or digitally manipulated in a manner that would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of the individual or replace an individual’s likeness with another individual and depicted in the recording.”

Note the following about this law:
- For the second time, the word deepfake appears in the title of a law.
- The scope is limited to “audio or visual media,” without reference to the text (which is explained by the fact that this is a law restricted to the creation of deepfakes involving minors).
- There is no reference to AI (only “digitally manipulated”).
- The assumption that this is false content is made clear by the expression “would falsely.”

4.5. Minnesota

Since August 1, 2023, the bill approved by the Minnesota House of Representatives entitled “Cause of action for nonconsensual dissemination of deep fake sexual images established, crime of using deep fake technology to influence an election established, and crime for nonconsensual dissemination of deep fake sexual images established” (HF 1370) has been part of the Minnesota Statutes.

The law describes “Deep fake” as “any video recording, motion-picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof: (1) that is so realistic that a reasonable person would believe it depicts speech or conduct of an individual; and (2) the production of which was substantially dependent upon technical means, rather than the ability of another individual to physically or verbally impersonate such individual.”

Note the following about this law:
- The word ‘deep fake’ (again, in two words) also appears in the title of the law.
- The law is comprehensive, although it does not directly refer to the issue of the text (only indirectly, through the expression “any technological representation of speech”).
- There is no reference to AI and the wording found seems very vague: “technological representation” and “the production of which was substantially dependent upon technical means.”
- Although reading the text leaves no doubt that it addresses false content, there is no direct reference to this assumption. In Subd. 2. (“Nonconsensual dissemination of a deep fake”) it reads that “(2) the deep fake realistically depicts any of the following: […] (ii) artificially generated intimate parts presented as the intimate parts of the depicted individual.”

A final note: Although legal issues go beyond the scope of the investigation, it should be noted that this is the first law that mixes the fight against non-consensual pornography with electoral deepfakes.

5. Discussion

We summarise the main points of this research (=Q3) in the Table 2:
Table 2. Summary of the research.

<table>
<thead>
<tr>
<th>Law</th>
<th>Date</th>
<th>In the title</th>
<th>In the text</th>
<th>Media referred</th>
<th>Fake/false</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DF</td>
<td>SM</td>
<td>DF</td>
<td>SM</td>
</tr>
<tr>
<td>SB 751</td>
<td>9/01/19</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>SB 309</td>
<td>6/23/21</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>SB 5152</td>
<td>7/23/23</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>SB 175</td>
<td>8/1/23</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>HF 1370</td>
<td>8/1/23</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

(DF: deepfake; SM: synthetic media; AI: Artificial intelligence; Fake/false refers to the direct use of the words in the legal texts)

Source: Own elaboration.

Of the five laws that constitute the sample, three were approved in 2023 (second semester).

This highlights, first of all, the pioneering spirit of the Texas law that was passed in 2019. As it is visible, if the word deepfake fearfully appears in the Texas law, then it becomes normal, including its use in titles.

However, the evolution is most notable in the supports that are being contemplated over time: what started only with video is now extended to a variety of other supports but not to the point of expressly including the text.

Of the five laws, there is one that stands out for being different: the Washington legal diploma is the only one that does not use the word deepfake, preferring instead the expression synthetic media. But what makes it especially different is the explicit reference to AI, accompanied by the word “false” (image, audio or video). It is the only one of the five laws that does so.

### 6. Conclusions

This investigation aimed to answer three questions: How can the concept of deepfakes be characterised? (Q1); Has the concept of deepfakes evolved over time? (Q2); What are the decisive elements upon which to build the concept? (Q3).

With regard to Q2, it seems clear to us that the concept has evolved over the six years (2017 – 2023), mainly through the diversification of media supports that can be created through AI: if in the beginning, it was just video, today there are already several definitions that do not forget the text in addition to image/photography and audio. None of the analysed state laws, however, foresees the possibility of the text being a deepfake.

To build the concept (Q3), it is therefore necessary to consider:

- i) Video, photography, audio and text. This does not mean that they are or could become the only ones, but they are fundamental at this point. However, so that the laws do not become outdated or at least ‘incomplete’ (as manifestly happened with the Texas law, for example), a generic and comprehensive formulation on the supports would be more adequate. To prevent the laws from becoming outdated because we limit the supports to the means known at any given time, as we saw with the Texas or even Hawaii laws, the use of an expression such as “[…] or other media” to the supports that are intended to enunciate (video, image/photo, audio, text) could solve the problem.

- ii) A reference to AI, whether generic or relative to any of the specific AI techniques (machine learning, deep learning, generative adversarial networks, artificial neural networks, generative artificial intelligence etc.). There are only deepfakes using AI and there are only deepfakes because there is AI. Failure to include this element could mean that a photo altered by Photoshop or a video that has been subject to special effects (or simple editing, such as cheapfakes) can be considered deepfake, with all the mistakes that can be guessed. At this moment the AI-powered language models capable of generating human-like text, images or videos based on context and past conversations, like the one
developed by OpenAI (ChatGPT) are the ‘state of the art’. Can anti–deepfake laws serve to limit the malicious uses of these AI–powered language models? It is important to bear in mind that ChatGPT both produces false and true content (or, in some cases, mixing true with lies or at least inaccurate information).

- iii) It seems crucial to us that the definition, particularly in legal terms, includes a reference to the idea of fake or false. In other words, when a deepfake is created, its genesis is based on the assumption that it is false, either partially or totally. What we saw in the analysis of the five laws is that only two expressly declared it, while the remaining three left it implicit, with varying degrees of effectiveness. In addition to the advantages that are foreseen in having a law be as clear as possible, the introduction of the ‘fake/false’ element has another merit: It will exempt much content that is also created by AI but which does not have objects to manipulate (in art, medicine, education, satire, etc.; see Ackerley, 2023; Epstein, 2023; Stock, 2023 or Wen et al., 2023). For the non–legal purposes of this investigation, we did not use the idea of ‘malicious’ as a distinctive criterion for defining deepfakes; for the legal context, it seems fundamental but, in general, deepfakes live beyond this specific universe. A deepfake can be false/fake (all are...) without being malicious. Likewise, it is not because it is generated by AI that it becomes malicious. And, as an example, “been intentionally manipulated” (Washington law) could be a deepfake of a video song or any innovative medical therapy.

- iv) Finally, is it possible to build a definition of deepfake without using the word? As this work demonstrates, several state laws in the U.S. claim to be anti–deepfake laws without ever using the word. It seems to us that this only serves to generate misunderstandings. There is, however, an alternative, as the Washington law shows, which is the use of the expression synthetic media. Basically, it is possible to apply the phrase “Fake/manipulated content in video, image, sound or text, generated by AI” to the word ‘deepfake’ or to the expression synthetic media.

Based on the four assumptions set out to respond to #Q2, it is thus possible to characterise the concept of deepfakes (≡Q1) even though it is clear that “legislators have struggled with the appropriate definition of deepfakes and synthetic media [...] and only time will tell if they can craft a definition that both is appropriately broad to capture all the different kinds of media that can be produced” (Ferraro apud Coyers, 2023).

It is essential to bear in mind that if no definition is immutable, matters that relate to a technology in constant evolution (“still in flux,” according to Vincent [2018]) and that ‘learns by itself’ (machine learning) become more precarious (Barr, 2022; Fernández, 2020).

In addition to wanting to systematize the various elements that make up the deepfake concept, this research showed the importance of not ignoring what has been the most forgotten element, both among lawmakers and the scientific community, the text. The explosion of generative AI tools only highlights the importance of not ignoring text. Although the issue is beyond the scope of this work, the difficulties that scientists and technological companies have demonstrated in finding effective ways to combat deepfakes are known. At this stage, and in the absence of better solutions, the dissuasive power of laws seems to be one of the most effective ways.

In short, and returning to the beginning, no other area is as sensitive to the need to clearly define the objects in which it intervenes as legislation. A law can be created with a certain objective and its application fails because it is poorly configured. With this investigation, we intend to help find better solutions.

Even taking into account the basic principle of Amara’s Law (Wikipedia, 2022) according to which we tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run, the only invalid alternative is to do nothing, if, as Bill Gates (2023) says, “Deepfakes and misinformation generated by AI could undermine elections and democracy.” And if laws are not the only way to combat malicious deepfakes, they will
certainly play a relevant role, without which the fight will be more difficult. But, as Westerlund (2019) stated, “In order to fight against deepfakes, we need to understand deepfakes.”

The author declare that he is free from any personal or commercial association and that there isn’t a conflict of interest in connection with the submitted article.

References


Ackerley, B. (2023). We need to accept that deepfakes are here to stay in film and TV. New Scientist. Retrieved from https://www.newscientist.com/article/mg25734240-800-we-need-to-accept-that-deepfakes-are-here-to-stay-in-film-and-tv/


Meneses, J. P.

Seeking to define deepfakes from U.S. state laws

HB 0085. (2021). An act relating to crimes and offenses; creating an offense for the nonconsensual dissemination of an intimate image; specifying elements and penalties of the offense; providing definitions; providing exemptions; and providing for an effective date. Wyoming House Bill. Retrieved from https://legiscan.com/WY/bill/HB0085/2021


