Analysis of the criminal liability of the creators and propagators of "*deep fakes*" in the brasilian legal system

https://doi.org/10.56238/sevened2024.014-011

Bruno Moraes Alves[1], Ana Karen Vasconcelos Araújo[2], Juan Fonteles Cavalcante[3], Francisco Expedito Galdino Júnior[4], Luiz Henrique Lopes Rodrigues[5] and Pedro Hygor Soares de Oliveira[6]

ABSTRACT

The present work has as its object the investigation about the criminal responsibility of the creators and disseminators of "deep fakes", which is a technology used to tamper with videos. This technology has been used to commit several crimes, such as tampering with evidence, spreading fake news, revenge pornography and the practice of crimes against honor, and it is important to find out if Brazilian law already has effective means to curb such conduct or if it is necessary to create an autonomous crime to punish the practice of "deep fakes". The method of approach used for the preparation of this work was deductive, and the research technique adopted was bibliographic, through the analysis of books, articles, news and legislation in the fields of Criminal Law and Digital Law. The conclusion reached was that, although there is no specific provision criminalizing the practice of "deep fakes", they are used as a means of executing other crimes, so that it is not necessary to create an autonomous crime just to criminalize such conduct. On the other hand, considering that the feeling of anonymity of the internet, added to the difficulty in punishing such crimes, make criminals feel encouraged to practice "deep fakes", it is essential to issue a qualifier or cause for increased punishment for crimes committed through these technologies. Regarding the responsibility of the propagators of these fake videos, it is necessary to analyze whether the crime committed through this technology contemplates, in its text, the possibility of punishing its disseminators as well. If the answer is affirmative, it will be possible to hold the propagator of the "deep fake" responsible not only for the crime committed, but also for the qualifier/cause of increased penalty related to the use of this technology for the practice of the crime.

Keywords: Deep fakes, Fake News, Cybercrimes, Artificial intelligence.

[1] PhD in Law from the Federal University of Santa Catarina – UFSC, Full Professor at Faculdade Luciano Feijão
E-mail bruno_ma@hotmail.com

[2] Postgraduate student in Labor and Social Security Law at Faculdade Luciano Feijão – FLF, Faculdade Luciano Feijão
E-mail karenvasconcelosadv.ce@gmail.com

[3] Post-Graduate Student in Labor and Social Security Law at Faculdade Luciano Feijão – FLF, Faculdade Luciano Feijão
E-mail juanfontelesadv@gmail.com

[4] Post-Graduate Student in Labor and Social Security Law at Faculdade Luciano Feijão – FLF, Faculdade Luciano Feijão
E-mail expeditogaldino@gmail.com

[5] Post-Graduate Student in Medical and Health Law at Faculdade Legale – FALEG, Faculdade LEGALE, Rua da Consolação
E-mail: luizlopes100@gmail.com

[6] Law student at Faculdade Luciano Feijão – FLF, Faculdade Luciano Feijão
E-mail pedrohygor03@gmail.com

INTRODUCTION

The global population is witnessing the Fourth Industrial Revolution, which has as some of its protagonists artificial intelligences, software and nanotechnology.

One of the products of this technological advance was the creation of "deep fakes", which consist of using artificial intelligence to tamper with videos, adding faces or speeches different from the originals, thus simulating the truth.

The aforementioned technology, which at first had as its main purpose the satire of certain individuals or situations, is increasingly being used for illicit purposes, among which we can mention the creation and propagation of "fake news" in times of elections and war, "sextortion", "catfishing" and the tampering of means of evidence. in order to affront several rights provided for in the Constitution, such as the right to honor and image.

In the current national system, there is no express legal provision that criminalizes, by itself, the creation or dissemination of "deep fakes". However, there are certain situations foreseen as a crime that can be practiced using "deep fakes" as a means of execution. In this sense, it is necessary to analyze the circumstances of the specific case, in order to observe whether the conduct practiced through the "deep fake" conforms to any crime, and the principles of the prohibition of analogy harmful to the defendant in criminal law and the prohibition of deficient protection must always be observed.

The first topic is dedicated to making a summary of the industrial revolutions throughout history, up to the present moment, in which the Fourth Industrial Revolution is lived. In addition, it also takes care of conceptualizing cybercrimes, their species and main characteristics.

The second topic, in turn, is intended to address the emergence and popularization of "deep fakes", through the phenomenon of "fake news", analyzing the harm that this technology has brought and the way the national legal system deals with this issue, in order to discuss the need to create its own legislation to curb such conduct.

Regarding the methodology, the bibliographic research was used, through the analysis of books, articles and laws and news related to computer relations and criminal law, using the deductive method.

Through the analysis and discussion of the topics brought up in the mentioned topics, the general objective of this work is to investigate how the agents who create and propagate "deep fakes" can be held criminally responsible in BRASILian law, discussing the need – or not – to create specific legislation to punish this type of crime.

CYBERCRIME

The Fourth Industrial Revolution brought about several changes in society's way of life, especially with the development and improvement of artificial intelligence.

This change in the social structure has brought numerous effects, both positive and negative. Among the negatives, the proliferation of crimes committed through – or against – computer systems, called "cybercrimes", deserves to be highlighted.

Because of this, this topic addresses the revolutions faced by society until we reach the current moment: the Fourth Industrial Revolution, as well as the importance of adapting criminal law to face virtual crimes, classifying them and analyzing their characteristics.

THE FOURTH INDUSTRIAL REVOLUTION

Society is constantly changing, always seeking to create new ways to facilitate work and community life. Because of this fact, humanity has developed, throughout history, several mechanisms, which have brought about profound changes in the social structure of their epochs.

Today's society is experiencing what Schwab (2016) calls the "Fourth Industrial Revolution", whose main characteristic is the improvement of artificial intelligences and nanotechnology:

> Some of these innovations are in their 'infancy' phase and have not yet shown their full potential. The fourth industrial revolution is not defined by each of these technologies in isolation, but by the convergence and synergy between them. (ROSA, 2019, p. 07).

A striking development of this revolution is the digitalization of labor relations. Whether in e-books, taxi apps – such as Uber – or music – such as Spotify – the reality is that, increasingly, society has the most diverse products and services available only with access to the internet. (AIRES; MOREIRA; FREIRE, 2017)

This digitalization of human relationships ended up creating a new face to social life: the virtual dimension, or disruptive dimension. According to Lima Filho (2021, p. 221), in this dimension: "Humans and machines work in such a close and similar way, that sometimes it becomes difficult to restrict certain activities as exclusive to only one of the two, rejecting the other."

The Fourth Industrial Revolution differs from the others by three important aspects: the speed of diffusion of its products; its profundity, since this revolution modifies not only the form of production of the market, but also involves political, economic and social issues; and its systemic impact, as it implies a complete transformation of society. (SCHWAB, 2016)

Regarding the speed with which the inventions of this revolution spread, Harari (2017, p. 375) asserts:

> In the last two centuries, the pace of change has become so rapid that the social order has acquired a dynamic and malleable character. It now exists in a state of permanent flux. When

> we talk about modern revolutions, we tend to think of 1789 (the French Revolution), 1848 (the liberal revolutions), or 1917 (the Russian Revolution). But the fact is that, these days, every year is revolutionary. Today, even a 30-year-old can honestly say to unbelieving teenagers, "When I was young, the world was completely different." The internet, for example, only became widespread in the early 1990s, a little over twenty years ago. Today we can't imagine the world without it.

As noted, the Fourth Industrial Revolution brought about a profound change in the social structure of the whole world.

The development of these technologies, especially artificial intelligence and nanotechnology, has brought numerous benefits to society, such as easier access to various products and services, "autonomous vehicles, 3D printing, nanotechnology, biotechnology, materials science, energy storage, and quantum computing" (SCHWAB, 2016, p. 15), among other innovations.

However, the improvement of these techniques, as well as the development of the virtual dimension in the lives of individuals, has opened the door to a new kind of crime: cybernetic, which will be the object of study in the following topics.

CHARACTERISTICS OF CYBERCRIME

Cybercrimes, also known as "computer crimes" or "virtual crimes", are those committed through or against computer technologies.

In this sense, computer crimes are conceptualized as being "any typical, anti-legal and culpable action practiced by an individual or legal entity, with criminal use involving data processing and/or data transmission, without the need for an internet connection." (MAUÉS; DUARTE; CARDOSO, 2018, p. 171)

As a result of the numerous ways in which information technology can be used in these crimes, cybercrimes can be divided into proper and improper crimes, and there are authors who even admit the existence of the mixed modality, such as Lima Filho (2021).

Own crimes, also called "pure" crimes, are those in which the objective for the commission of the crime is to damage the technology itself. This means that, when it comes to this type of crime, the criminal legal asset to be protected is information technology itself. (LIMA FILHO, 2021)

Lacerda and Silva (2021, p. 15) exemplify conducts that can be considered cybercrimes: "As crimes of their own, there are examples of viruses that invade systems to destroy information, steal information, or even damage the device, be it smartphones, computers, or tablets."

On the other hand, improper or impure cybercrimes are those in which the animus of their perpetrator is not the attack on information technology, but rather a different crime, provided for in the legal system. In this type of crime, the computer system is not the "victim", but rather the means of execution of the crime. (LIMA FILHO, 2021).

Various kinds of crimes can be committed through technology. Lacerda and Silva (2021, p. 15) cite some examples of crimes committed by this means:

> Improper crimes, on the other hand, include a wide range, such as inducing, instigating or assisting suicide or self-mutilation carried out through computer networks and dissemination of a rape scene or rape scene of a vulnerable person, sex scene or pornography by any means of mass communication or computer or telematic system.

An observation should be made: the examples listed by the authors contemplate only crimes in which, in their own wording, there is a provision to be committed through the computer network. However, there is also the possibility of other types of crimes being committed through the internet.

An example would be crimes against honour, such as slander, defamation and slander, provided for in Art. 138 to 140 of the Penal Code (BRASIL, 1940). These crimes do not have in their conceptualization the fact that the conduct is practiced through the internet, nor do they list any qualifier or cause for increased punishment resulting from their practice through this platform. However, it is perfectly possible to admit to committing a crime of, for example, defamation, through social networks.

The fact that an individual publishes a certain post containing knowingly false information about another, and that degrades his or her reputation, is considered a crime of defamation, and, in this case, it would be a defamation practiced through the internet, being, therefore, an improper cybercrime.

This form of cybercrime can also be called "common cybercrime", since it is the practice of common crime, in which information technology is only a form of execution of the crime, not reaching the core of the criminal type. In this regard, the CPI on Cybercrimes provides:

> Common cybercrimes are those in which computer devices are used only as an instrument to carry out a crime already typified by the criminal law, constituting just one more means of executing these crimes, as occurs in the following crimes, already typified by the criminal law: embezzlement (art. 171 of the CP), threat (art. 147 of the CP - Penal Code), crimes against honor (articles 138 to 140 of the Criminal Code), the dissemination of child pornographic images (article 241-A of the Statute of the Child and Adolescent – Law No. 8,069/90), the crime of copyright violation (article 184 of the Criminal Code), among others. (BRASIL, 2016, p. 75)

It should be noted that, although in impure cybercrimes the main objective of the crime is to reach legal goods other than information technology, it can be indirectly harmed. Similarly, in pure cybercrime, although the main purpose is to injure computers, tablets, software, etc., other assets can be reflexively affected. (LIMA FILHO, 2021).

On this issue, Jesus and Milagre (2016, p. 53) assert:

> These classifications can merge, as, for example, in the crime in which a computer legal asset is assaulted so that the agent can commit the final crime, that is, assault another legal asset, or even in the case in which the aggression to the computer legal asset also affects other assets,

> even if they are not informatic. Let's imagine, for example, the hypothesis where the agent invades another person's device and alters information causing the person to be classified as wanted by the police. Greater damage may follow.

Examples of mixed cybercrimes would be "the illicit transfer of values in a "homebanking" or the practice of "salemislacing" (daily withdrawal of small amounts in thousands of accounts, also known as balance withdrawal). " (BRASIL, 2016, p. 75).

Leaving aside the issue related to the classification of cybercrimes, another important aspect regarding these crimes must be analyzed: the difficulties involved in curbing these behaviors and punishing their agents.

Three central points should be highlighted: the mutability of the techniques used in cybercrimes, the definition of the crime scene and the identification of its authorship. (LIMA FILHO, 2021)

The first obstacle pointed out is related to the dynamism inherent to the Fourth Industrial Revolution, since, as exposed, this revolution has as one of its central characteristics the speed with which technologies are developed and disseminated around the world. (SCHWAB, 2016)

Due to the speed with which information technology evolves, it is difficult for the Legislative Branch to keep up with such changes. This fact causes legislative gaps in the legal system, which often leads to the impunity of illegal conduct practiced through the internet or the computer system.

The second difficulty concerns the definition of the location of the crime in cybercrimes (LIMA FILHO, 2021), as well as which would be the competent authority to judge them. Unlike ordinary crimes, which occur in tangible reality, cybercrimes occur in another dimension: the virtual one. Because of this, it is not always possible to identify the place where the crime occurred, which makes it very difficult to apply the law to the specific case. (PIAIA; COAST; WILLERS, 2019)

An example can be given: if an individual, in BRASIL, commits a crime of embezzlement against a person who is in Chile, using his cell phone, what would be the law applied? And which state would be competent to apply this law?

The principle of territoriality, adopted by the BRASILian Penal Code, in its article 5, provides: "BRASILian law shall apply, without prejudice to conventions, treaties and rules of international law, to the crime committed in the national territory." (BRASIL, 1940).

Thus, if a conduct, considered a crime, is practiced in BRASILian territory, the agent provocateur of this crime must be judged in accordance with BRASILian criminal law.

It is also possible to apply BRASILian law to crimes that did not occur in BRASILian territory, hypotheses called by the Penal Code "conditioned extraterritoriality". In these cases, it will be necessary to comply with the requirements established in article 7 of the Penal Code in order to apply BRASILian law to a crime committed abroad. (GRECO, 2017)

However, when it comes to crimes committed through computer networks, it is difficult to understand which law would be applicable in each specific case. On this topic, Pinheiro (2021, p. 43) asserts:

> Some other principles of Law should be rethought within the scope of Digital Law, such as the principle of territoriality. Where is the door? How far does a legal system reach? The problem is not only in the realm of the Internet, but in every globalized and convergent society, in which it is often not possible to determine the territory in which the legal relations, the facts and their effects took place, making it difficult to determine which norm to apply using traditional parameters.

Article 6 of the Penal Code, when dealing with the place of the crime, adopted the theory of ubiquity, according to which "the crime is considered to have been committed in the place where the action or omission occurred, in whole or in part, as well as where the result occurred or should have occurred." (BRASIL, 1940)

This means that, if there is someone, "in the State of Rio de Janeiro, who invades someone else's computer, located in São Paulo, we would have the court where the invaded device is competent to prosecute and judge the computer crime". (JESUS; MILAGRE, 2016, p. 61)

With regard to the authority competent to try crimes, the Code of Criminal Procedure states that "Jurisdiction shall be, as a rule, determined by the place where the offence is committed, or, in the case of an attempt, by the place where the last act of execution is committed." (BRASIL, 1941)

From what can be understood from the analysis of the article transcribed above, bringing it to the context of digital crimes, it is observed that the competent authority to judge the crime will be that of the place where the result of the crime occurred – or should have occurred. Thus, using the previous example, if a person who is in BRASIL commits a crime against an individual located in Chile, using his cell phone, the competent country for the trial will be Chile, as it is the place where the damage occurred or should occur.

It is interesting to note the caveat that Jesus and Milagre (2016, p. 61-62) make regarding the possibility of a crime being committed in a certain territory, but with the origin of the connection masked:

> With regard to illegal conduct practiced in foreign territory, BRASILian rules would not apply, considering the country's sovereignty, and the issue should be dealt with by extradition. Logically, the BRASILian authority is competent to prosecute a digital crime committed by a BRASILian agent abroad, with a victim in BRASIL, but it will depend on this agent entering national territory. Therefore, crimes committed through proxies, vpns, among other resources to mask the origin of the connection, where the agent is in BRASIL and only uses a connection from abroad, can be prosecuted here, provided, of course, that the criminal is identified. And therein lies another problem, as foreign providers often refuse to provide access data to applications made by BRASILians, but stored abroad.

Finally, another major difficulty that exists in relation to the punishment of digital crimes is the difficulty in identifying who is the perpetrator. Many individuals use anonymous or even fake profiles to cause cyberattacks, which makes it difficult to criminally investigate this type of crime.

The solution currently found to reach the perpetrator of cybercrimes is to track the machine's IP, which would correspond to the address where the computing device in question is located.

It should also be noted that Law No. 12,965/14, also known as the "Civil Rights Framework for the Internet", imposes on internet providers the obligation to keep access records – IP addresses of machines – for a specific period of time. (LIMA FILHO, 2021)

From what has been exposed in this chapter, it can be observed that the Fourth Industrial Revolution caused the evolution of computer technologies, which led to several changes in the social structure, both positive and negative.

One of these changes was the spread of cybercrimes, which still face difficulties in the field of criminal law enforcement in our legal system.

THE CRIMINAL LIABILITY OF THE CREATORS AND DISSEMINATORS OF *"DEEP FAKES"*

The virtual environment, in addition to giving rise to the creation of new types of crimes, typical of its environment, also made preexisting behaviors gain a new dimension, even greater than the physical one. In this context, *"fake news"* has spread, gaining greater popularity among Internet users. Subsequently, technological mechanisms were created that transformed *"fake news"* into something even more credible and dangerous – "*deep fakes*".

In this topic, the origin and dangers that *"fake news"*, especially *"deep fakes"*, can cause to society will be addressed. At the end, an analysis will be carried out on the sufficiency – or not – of the current BRASILian legislation in combating these conducts.

THE ADVENT OF *"FAKE NEWS"*

"Fake news" is, as its name suggests, untrue information. With the advent and popularization of the *internet*, especially social networks, the spread of this false information has gained an even greater dimension.

Previously, the dissemination of news was restricted to newspapers and magazines, with quality control parameters, in order to ensure the veracity of the information disclosed. On the other hand, nowadays, anyone with access to the *internet* can publish a news story. Similarly, individuals connected to the website on which the information was published may have access to it, regardless of whether the news is true or false.

This practicality that technological means have brought means that, increasingly, the *internet* is scrapped with more information.

The problem lies in the fact that this information is not always true. However, although this is not true data, most individuals who access this information do not take the necessary precautions to verify their sources, ending up believing that what is reported is reality. (EARTH; ORSINI; ABREU, 2021)

A recent example of the harmfulness of "*fake news"* was what happened at the height of the COVID-19 pandemic in BRASIL. At first, news was spread that the virus would not be as harmful as the newspapers claimed, which caused people to not properly comply with the necessary social isolation. Subsequently, with the manufacture of the vaccine, more false information spread, this time claiming that the coronavirus vaccine would be harmful to health, which led to a delay in vaccination against the virus. (EARTH; ORSINI; ABREU, 2021).

The result of the massive spread of this fake news could not be different: "in April 2019, BRASIL recorded the highest moving average of deaths due to covid-19: about 3 thousand daily deaths". (AFTER, 2021).

Faustino (2018) argues that technological development has led to a greater need on the part of the population to stay informed more and more quickly, which causes, on the one hand, the demand for information to grow and, on the other, the commitment to the reality of the facts to fall. This is because individuals no longer have the time – or the will – to check if the facts they are reading correspond to reality. The simple fact of "being on top of" the main news is enough.

Based on this thought, Faustino (2018) affirms the existence of a link between *"fake news"* and "post-truth" – a term considered, in 2016, by the Oxford Dictionary, as the word of the year – the former being a kind of the latter. Post-truth would correspond to the motives behind *"fake news"*, corresponding to the realization that the majority of the population cares less about the objective reality of the facts than how that news supports their personal beliefs and motivations. A fake news story about a certain pronouncement of a candidate would be motivated by political objectives, for example.

Fake news is a recent reality, existing since the moment of human evolution when individuals began to be able to communicate, and since then they can choose between telling the truth or a lie. (NOHARA, 2018, *apud* FAUSTINO, 2018)

Such a practice was perfected in Classical Antiquity, along with politics and rhetoric. At that time, "fallacies" were developed, which consisted of arguments that, according to logical development, should be considered correct, but which were, in reality, a kind of "logical lie", having errors in their structure, being used to cause injury to their opponent. (SANTOS, 2015)

Although the act of spreading fake news is not a recent creation, it was only in 2016 that the term *"fake news"* hit the news around the world, with the United States presidential elections. At the time, a lot of false information was disseminated, especially on social networks, about the candidates running for government positions. (EARTH; ORSINI; ABREU, 2021)

In this way, "*fake news* has gained several nuances, such as for electoral purposes, through the *firehouse of falsehood,* fraud or simply disinformation for disinformation's sake, such as whatsapp chains." (FURBINO; SOUZA, 2021, p. 45)

"Fake news" can be classified into three categories, according to its purpose. In this way, fake news can be intended to: a) divert the population's attention from the real problem – in this case, untrue information is released on the *internet* to distract individuals, causing them not to pay attention to relevant and real problems; b) promote a particular candidate to the detriment of others; and c) to overwhelm the reader with a large amount of information, so as to make him have no notion of what is reality and what is a lie. (ESTABEL; LUCE; SANTINI, 2020, *apud* TERRA; ORSINI; ABREU, 2021)

In BRASIL, there is no specific criminal type that tries to criminalize *"fake news"*, and there is only, depending on the case, a framing of this conduct in crimes against honor. (FURBINO; SOUZA, 2021).

> Currently, anyone who spreads false information can be punished by federal laws that make no reference to the internet. They are the Penal Code of 1940, which deals with libel, slander and defamation, the Electoral Code of 1960, which already provides for penalties for the dissemination of untrue information, and the National Security Law of 1980, which establishes punishments only for those who spread rumors that cause panic in society. (GRIGORI, 2018)

However, there are bills in progress that aim to punish the creators of *"fake news"*. "Until 2018, there were 20 PLS imposing penalties on fake news creators, penalties ranging from R$1,500.00 (one thousand five hundred reais) in fine to 8 years in prison." (GRIGORI, 2018)

In the civil area, Bill No. 7,604/2017 proposes to add an article to Law No. 12,965/2014 (Civil Rights Framework for the Internet). The purpose of this provision would be to attribute to internet access providers the responsibility for fake news published on their domains. (FAUSTINO, 2018). However, this article violates the provisions of article 19 of the same law, which provides that the provider can only be held liable for content published on its *websites* if, after receiving a court order to remove the content, they remain silent. (BRASIL, 2014)

In the criminal sphere, Bill No. 437/2017 suggests the inclusion of a new type of law in the Penal Code, which would correspond to the crime of "dissemination of false news". (FAUSTINO, 2018). The wording of such an article would be as follows:

> Article 287-A - Disseminate news that you know to be false and that may distort, alter or corrupt the truth about information related to health, public safety, the national economy, the electoral process or that affects relevant public interest.

> Penalty – imprisonment, from six months to two years, and a fine, if the act does not constitute a more serious crime.
> § 1 If the agent practices the conduct provided for in the caput using the internet or any other means that facilitates the dissemination of false news:
> Penalty – imprisonment, from one to three years, and a fine, if the act does not constitute a more serious crime.
> § 2 The penalty is increased from one to two thirds if the agent disseminates the false news to obtain an advantage for himself or for others. (BRASIL, 2017)

As can be seen from the reading of the article, it would be required, in order to be classified as a crime, prior knowledge that the news disseminated is false. In this case, if an Internet user shares false news, but believes that this news is true, they would not be committing any kind of crime. Thus, "applying terms characteristic of the criminal sciences to the study of *fake news*, the subjective element of the type of *fake news* is in the conduct of reproducing information that is known to be false on the part of the person who writes it." (WALDMAN; HORAS, 2018, p. 343)

Waldman and Horas (2018) criticize the creation of a new criminal type just to criminalize *"fake news"*, stating that a solution should not be sought in the creation of new crimes, since the conduct of disseminating false information would already be framed in existing crimes – such as crimes against honor. According to the author, the main concern should be to find practical instruments to curb and punish these behaviors in the virtual environment.

Bill No. 215/2015, on the other hand, does not seek to create a new type, nor does it mention the term *"fake news"*, but brings a cause for an increase of 1/3 of the penalty for those who commit the crimes of libel, slander and defamation through the *internet*. Currently, this is the Bill that is in the most advanced phase, awaiting presentation to the Plenary of the National Congress. (GRIGORI, 2018)

From the above, it is observed that *"fake news"* has been causing several ills to society, and there are even bills with the objective of punishing the authors of this practice.

However, over time, the way of practicing *"fake news"* has evolved, leading to the creation of *"deep fakes"*, which are the subject of the next topic.

"DEEP FAKE": QUALIFIED "FAKE NEWS"?

The evolution of technology, especially artificial intelligence, has culminated in the creation of *"deep fakes"*, which consist of the distortion of videos and images in order to mask the truth and simulate events that never occurred, which often ends up violating the honor and image of individuals who have their image used without consent.

The use of artificial intelligence for this practice was originally called *"fake video"*. However, because it became popular thanks to a Reddit user, who called himself "*deep fake"*, this term became the name used for this type of technology. (MEDON, 2021).

According to Faustino (2018, p. 108): "The term *deep fake* arises precisely because of the union of the term *deep*, taken from the concept of *deep learning,* and the term *fake* from *fake news".*

"The term then came to be associated with this technique, which operates the fusion of moving images, generating a new video, whose degree of reliability is raised to a level that only with great attention can be noticed that it is a montage". (MEDON, 2021, p. 262)

At first, the aforementioned technology was mainly aimed at the film industry, being used for various functions, such as changing the face of stuntmen for the face of the main actor, special effects, etc. In this sense, Medon (2021, p. 269) teaches:

> The film industry has also made use of this technique. One of the most famous cases was perhaps that of the film *Rogue One: A Star Wars Story* (2016), from the homonymous series, when some characters were recreated. The most peculiar was, without a doubt, that of *Commander Tarkin*, played by the British Peter Cushing, as this actor had already passed away in 1994. Using computational techniques, the so-called "digital reconstruction" of the image of the deceased actor was made possible, which raises questions, such as the need for authorization from the heirs for the reconstruction of his image. It should be noted, however, the peculiarity of this situation: it is not a question of reproducing images captured in the past, but of creating new images, based on previous captures.

As noted, at first, the purposes for which the *"deep fakes"* were intended were completely lawful, aiding in the production of artistic works. However, with the passage of time, the technology became popular and improved, gaining space in the humorous field, which is why it began to be used to satirize individuals and situations.

The use of *"deep fakes"* for satire, in itself, already raises questions about its legal repercussions, given that, depending on the concrete situation, it can offend the dignity of the people who appear in the videos.

However, with the passage of time, *"deep fakes"* are increasingly being used for unquestionably illicit purposes, such as the tampering of videos of candidates, in order to manipulate the results of elections; the insertion of the faces of actresses in pornographic videos; the creation of fake profiles for the commission of crimes and the tampering of means of evidence.

An example of how *"deep fakes"* can influence the political arena through the spread of fake news can be seen below:

> Another example comes from a video made by an American comedian, using this technology, to warn people about its dangers, in which former U.S. President Barack Obama appears speaking badly about then-President Donald Trump, based on a fusion of moving images of Obama himself, associated with the comedian's voice, which imitated the former president. In the video, the alleged Obama calls Donald Trump a "total and complete idiot." The perfection of the montage is capable of leading inattentive people to the unshakable certainty that it was a real communication from Obama. (MEDON, 2021, p. 261)

We can also mention the recent publication of a *"deep fake"* by Volodymyr Zelensky, current president of Ukraine, a country that is at war with Russia, in which he appears announcing surrender to the Russian army. (WAKEFIELD, 2022).

It is noted, therefore, that the use of artificial intelligence for the creation of *"deep fakes"* can have catastrophic impacts, being able to totally influence the political scenario and the security of a State, putting democracy itself at risk.

In addition, the improvement and diffusion of *"deep fakes"* has also aided in the practice of revenge porn. "According to research released by Deeptrace in September 2019, 96% of *deepfakes* existing at the time were pornographic, with 100% targeting women when the content was pornographic." (MEDON, 2021, p. 261).

It is common knowledge that today's society, despite the advances, is still established on an eminently patriarchal structure, where the culture of machismo plagues the lives of millions of women around the world.

Revenge porn, or *"revenge porn"* is a reflection of this culture, consisting of the publication of videos of sexual content without the consent of the person in the video – largely female – as a form of retaliation for a certain event.

This behavior, already practiced before the popularization of *"deep fakes"*, has been further aggravated by the use of this technology – now the authors of revenge porn not only publish sexual videos without the consent of the other party, but can even create videos simulating sexual scenes that never occurred.

Faustino (2018) considers "deep fakes" to be a kind of "*fake news"*, since *"deep fakes"*, like *"fake news"*, have the objective of spreading false information, the former being an improved version of the latter.

This technology is, therefore, even more dangerous than traditional *"fake news"*, since, due to their sophistication, *"deep fakes"* end up looking much more real, giving a greater degree of credibility: it is much easier to suspect that a message or a text on a *blog* is fake than a video.

Due to the harm of such practice to society, it is necessary for the State to have mechanisms to curb and punish this conduct.

In view of this fact, the next topic will analyze whether the BRASILian legal system has such mechanisms or whether it is necessary to enact a specific law to regulate *"deep fakes"*.

IS THERE A NEED FOR LEGISLATIVE CHANGE?

From what is narrated, it is observed that the popularization of *"deep fakes"* has given new facets to the practice of various crimes, and it is necessary, therefore, to seek a way to criminally hold individuals who commit crimes through this technology criminally responsible, in order to ensure the protection of society in the face of this type of conduct.

However, because it takes place in a virtual environment, there are numerous difficulties for the criminal liability of the creators and broadcasters of these videos, such as the lack of specific legislation to regulate this type of crime and the difficulty of identifying the creators of the altered videos and the dimension that this content can reach.

The practice of "*deep fake",* by itself, is not considered a crime in the national legal system, leaving the question of how to criminally hold individuals who commit crimes through this technology criminally responsible.

In this context, there is a clash between two important principles of criminal law: the prohibition of deficient protection and the prohibition of analogy *in malam partem*.

The prohibition of deficient protection imposes on the State the duty to protect the fundamental rights of individuals and to ensure their application. Thus, the Government must not only refrain from violating the fundamental rights of its citizens, but must adopt positive conduct in order to protect them against attacks by third parties. (STEPHEN; BRITO FILHO, 2021)

The punishment of agents who commit crimes through *"deep fakes"* is not only a power of the State, but a duty, in order to guarantee democracy. In this regard, Da Costa (2011, p. 33-34) asserts:

> Miguel Reale Júnior points out that the correct application of Criminal Law and its sanctions constitute more than a right, a power of the State, which, aiming to ensure social harmony, cannot fail to act and leave its effectiveness to private individuals. If this were to be done, we would have a capitis diminutio, with the weakening of sovereignty and the emergence of a profound legal uncertainty for society, so that the effectiveness of the rule would be limited to the interest of the victim or his family, even generating legal uncertainty for the offender and for the State a limitation of the applicability of the law.

Thus, it is necessary to ensure that the rights provided for in the Constitution – such as the right to honor and image – are safeguarded against criminal practices, such as the use of *"deep fakes"* to violate such legal rights.

Regarding the prohibition of insufficient protection, Streck asserts (*apud* RUDOLFO, 2011, p. 117): "The prohibition of deficient protection can be defined as a structural criterion for the determination of fundamental rights, with the application of which it can be determined whether a state act - par excellence, an omission violates a fundamental right of protection."

On the other hand, it is necessary to observe that the BRASILian legal system, by enshrining, in article 1 of the Penal Code, the principle of legality, which provides that "there is no crime without a previous law that defines it, nor a penalty without prior legal sanction" (BRASIL, 1940), prohibits individuals from being punished for the practice of conducts not provided for by law as a crime.

From the wording of the aforementioned provision, two sub-principles were derived: that of legal reserve and that of the anteriority of the criminal law.

The principle of legal reserve provides that only a law in the strict sense can create new types of crime, and it is not possible, for example, to establish a new crime by decree. "Thus, only the law, in its formal and strict conception, emanating and approved by the Legislative Power, through an adequate procedure, can create types and impose penalties." (CAPEZ, 2011, p. 60).

However, the legal reservation of the incriminating criminal type does not empty its concept of the mere need for the existence of a criminal law in the strict sense to provide for a certain conduct as criminal, also requiring that the wording of the provision that establishes a new crime be clear and precise.

With regard to the principle of anteriority of the criminal law, it establishes that an individual cannot be punished for conduct that was not considered a crime at the time it was committed, even if there is a law that typifies such conduct as a crime. It is called "*tempus regit actum"* or "time rules the act". (CAPEZ, 2011)

In this way, the criminal law cannot retroact to harm the defendant, either to convict him for conduct that was not considered a crime when practiced, or to aggravate the penalty for a certain crime according to new legislation.

On the other hand, it is possible to apply a supervening criminal law to the crime committed before its enactment, provided that it aims to decriminalize the conduct or soften its penalty, under the terms of article 2 of the Penal Code. (BRASIL, 1940)

A corollary of this principle is the prohibition of analogy *in malam partem* in criminal law, consisting of the interpretation of a typical figure in an extensive way, in order to extend the scope of a given crime to other similar hypotheses, as exposed by Greco (2017, p. 177):

> The principle of legality also prohibits the use of analogy *in malam partim* to create hypotheses that, in some way, will harm the agent, either by creating crimes, or by including new causes of increased penalty, aggravating circumstances, etc. If the fact has not been expressly provided for by the legislator, the interpreter cannot use analogy in order to try to cover facts similar to those legislated to the detriment of the agent.*nullum crimen nulla poena sine lege stricta*).

It should be noted that the analogy can be divided into legal analogy, which occurs when the judge applies a law that regulates a certain situation to a similar case, and legal analogy, when general principles of law are applied to regulate a certain case in which there is no normative provision. (GRECO, 2017)

In view of the guarantee of non-removability of jurisdiction, a judge cannot avoid judging a given dispute using the premise of the non-existence of legislation that regulates the case. Thus, when the existence of a gap in the legal system is verified, it is necessary to resort to analogy, customs and general principles of law, as established by the Law of Introduction to the Rules of BRASILian Law (LINDB): "Art. 4 When the law is silent, the judge shall decide the case according to analogy, customs and general principles of law. (BRASIL, 1942). ”

Pinheiro (2021), when addressing the specificities of digital law, argues that, in this legal field, principles prevail over rules, given that technology evolves infinitely faster than legislative activity.

Due to the speed of this evolution, a legal problem arises: the lack of proper laws that regulate the specificities of the digital world. The solution found by digital law to resolve such an impasse, according to Pinheiro (2021), would be the use of analogy.

However, as mentioned, when we enter the criminal field, it is not possible to use analogy, customs or principles in order to harm the defendant, and therefore it is not possible to apply a certain criminal type to a similar hypothesis in order to punish a certain conduct.

It is necessary to analyze, then, whether in the national legal system there is the possibility of criminal liability of the creators and disseminators of *"deep fakes"*, because, otherwise, it will be necessary to create a new criminal type in order to criminalize such conduct.

As reported in the first topic of this work, there are two types of cybercrimes: proper and improper, and some authors admit the existence of a mixed type.

Cybercrimes themselves would be those in which the injured legal good itself is information technology; the improper ones are the crimes in which technology is used as a means to commit already existing crimes, and the mixed ones would be those in which information technology is, at the same time, the offended legal asset and the means of execution of another crime (LIMA FILHO, 2021).

In the case in question, it can be seen that the types of cybercrime that best fit the *"deep fakes"* would be the improper and mixed modality, depending on the situation. Note two hypotheses: a) A certain individual hacked into a third party's computer, obtaining for himself a random video of that person. Subsequently, he edited that video and superimposed the image of the victim's face on a pornographic video, publishing it on the *internet*; b) A certain individual, who already had lawful possession of a third-party video, edits this recording, superimposing the image of the victim's face on a pornographic video, and publishes it on the *internet*.

In the first case, the agent both invaded a computer device, thus committing a cybercrime of his own, given that he caused damage to the legal asset of computer technology, and an improper cybercrime, since he used technological artifices to edit the video and hurt the honor and image of the victim. It would be, in this case, a mixed cybercrime.

In the second case, on the other hand, the information technology was not harmed, being only a means for the practice of a certain crime, thus configuring itself as an improper cybercrime.

However, regarding the first situation, there is already a criminal type in our legal system to punish the conduct practiced against the computer system, that is, the crime of invasion of a computer device, provided for in article 154-A of the Penal Code, having been added by the Carolina Dieckmann Law. (BRASIL, 2012)

In this way, it would not be necessary to have a new criminal type for the punishment of the conduct of invading a computer device to practice a *"deep fake"*. The practice of *"deep fakes"* would therefore be an improper cybercrime, since it is only used as a means for the execution of other crimes.

In view of this, the question arises: should the procedure of creating *"deep fakes"* be prohibited, that is, should the technique used to edit these videos be criminalized?

The answer is no. Criminalizing the technique used to create *"deep fakes"* would be an inefficient solution, since, as explained, technologies have a much faster pace of change than the law. Thus, when a law criminalizing a certain technique was published, there would already be new ways of practicing that conduct, making the law completely ineffective (LIMA FILHO, 2021).

Thus, the most efficient solution, according to Lima Filho (2021), would be to criminalize conducts that can be practiced through this technology, and not the technology itself.

It is necessary, therefore, to ascertain whether there are already hypotheses of criminalization of conducts that can be practiced through *"deep fakes" in the BRASILian legal system*.

The legal assets that are harmed when a *"deep fake" is created and disseminated* are the image and honor of individuals. In the case of *"deep fakes"* related to pornographic content, the sexual dignity of the victims is also injured.

The BRASILian Penal Code, in its arts. 138, 139 and 140, already provides for the punishment of the individual who commits crimes against someone's honor, being divided into slander, libel and defamation.

Thus, it is not necessary to issue a new criminal type just to provide for the practice of such crimes through the use of *"deep fakes"*.

If someone edits a video in such a way as to make it appear that a certain person is committing a crime, the editor of the content will have committed the crime of slander (art. 138, CP). If, on the other hand, in the falsified video, the individual is not committing a crime, but is committing an act that discredits his or her conduct, the creator of the *"deep fake" will be* held liable for the crime of defamation (art. 139, CP). In the event that you injure someone through this technology, you will have committed the crime of injury (art. 140, CP).

Waldman and Horas (2018, p. 345), when commenting on *"fake news"*, argue that there is no need to create a new criminal type to criminalize such conduct:

> Bills that aspire to criminalize "fake news" treat the law in a simplistic way, so that the enactment of a new law is not of great value if it is applicable and efficient means to identify authors. If the criminal law already has the crimes of defamation, slander and slander, it would be the law so poor as to create a new incriminating criminal type for, specifically, the false news that is disseminated on the internet. Before the 2000s, when internet access was not so popular and accessible to BRASILians, the largest means of communication was television – according to the website brasil.gov is still predominant today (BRASIL, 2018) among BRASILians – there was no incriminating criminal type for fake news broadcast on television, taking into account sensationalist programs about crimes and news (gossip) about

> celebrities. Fake news has always existed in a society, the only change has been the channel it spreads.

From the above, it is observed that it is not necessary to issue a new criminal type just to criminalize *"deep fakes"*. However, it is certain that technology has greatly facilitated the practice of crimes against honor, as well as amplified their damage, since anyone can have access to the edited video, and not just people in the victim's social circle – as occurs when such crimes are not committed through the *internet*.

In addition, the difficulty in identifying offenders who commit crimes through computer networks means that there is an incentive to commit this type of crime, to the detriment of crimes that are not committed through information systems.

A possible solution to curb the practice of crimes against honor through the *internet* would be the creation of a qualifier or a cause for increasing sentences for individuals who use technology to carry out crimes.

It should be noted that there is already a similar provision in BRASILian law. Article 122 of the Penal Code, when dealing with the crime of inducing, instigating or assisting suicide or self-mutilation, provides, in its paragraph 4, that "the penalty is increased up to double if the conduct is carried out through the computer network, social network or transmitted in real time". (BRASIL, 1940)

The same solution could be applied in the case of *"deep fakes"*, with the provision of an increase in punishment or a qualifier in the case of crimes against honor or sexual dignity carried out using this technology.

Once the criminal liability of the creators of *"deep fakes"* is understood, the question arises: should the third parties who did not tamper with the video, but who shared it, also answer for the crime?

The answer to this question will depend on the type of crime committed through *"deep fakes"*. The crimes of defamation and libel do not include a provision for criminal liability for the propagators of false information.

On the other hand, the crime of slander, provided for in article 138 of the Penal Code, establishes, in its paragraph 2, that "the same penalty is incurred by those who, knowing the information to be false, propagate or disseminate it." (BRASIL, 1940)

In this case, two situations may exist: the first when a third party discloses information knowing it to be false, and the second when they share it in good faith, without being aware that it is a doctored video. In the first case, the agent will be punished with the same penalty as the creator of the false information. In the second situation, you will not be held liable.

The same reasoning may be applied in the eventual creation of a qualifier or cause for increased punishment for individuals who commit such crimes with the help of *"deep fakes"*: if they share the *"deep fake"* knowing that it is an adulterated video, they will be held responsible, including the qualifier/increase of the penalty. Otherwise, they will not be held criminally liable.

From the above, it was observed that, although there is no specific legislative provision that criminalizes the practice of *"deep fake"*, it is not necessary to issue a specific criminal type for this conduct, being due, however, the creation of mechanisms to increase the penalty of those who use such technology to commit other crimes, as well as of those who share such adulterated content knowing that it is false content.

CONCLUSION

The topic discussed in this work is extremely relevant for society in general and for the legal community, since *"deep fakes"* are increasingly present in society, affecting the daily lives of all individuals.

In the same way, it is relevant for the entire academic community, since the understanding of the causes and consequences of the dissemination of *fake news* and, in particular, *deep fakes*, raises several questions about the ethical limits of technology and its effect in various areas of law. It is also relevant in the field of sociology, as it has been found that the practice of certain crimes through *deep fakes* – such as, for example, "sextortion", affects a certain social group more than another.

Thus, detailed reflection on this topic is essential to understand its developments, in order to seek a way to hold accountable individuals who commit crimes through *"deep fakes"*, without, however, disrespecting the rules and principles in force in the national legal system.

The first topic provided an overview of the first, second and third industrial revolutions, also addressing the Fourth Industrial Revolution and its impacts on society. At the end of the chapter, it was concluded that this revolution, despite having brought numerous practical benefits to the global population, also led to the creation and popularization of cybercrimes. These crimes are growing every day, mainly motivated by three factors: the difficulty of identifying their perpetrators, the mutability of the techniques used, and the doubt about the definition of the crime scene. In addition, this type of offence can be subdivided into proper, improper and mixed computer crimes. The former correspond to those in which the violated legal asset is the information technology itself, while the latter are the type of cybercrime in which technology is used as a means to commit other crimes. The mixed, on the other hand, are a mixture of the two, where information technology is both the legal good affected and the instrument for the execution of the crime.

The second topic, in turn, addressed the characteristics of *"fake news"* and how they led to the emergence of *"deep fakes"*, exposing the dangers that this practice entails for society, such as the dissemination of fake news, sextortion and tampering with evidence, and also discussed the question of the need – or not – to create specific legislation to criminalize such conduct, in the light of the principles of prohibition of deficient protection and prohibition of analogy *in malam partem*. At the end of the topic, the conclusion reached was that, as predicted in the hypothesis of this work, *"deep fakes"* are a powerful means of execution for various types of crime, especially crimes against honor, but they are not, by themselves, a crime.

Despite this, it is not necessary to issue a specific criminal type just to criminalize such conduct, since, given the speed with which technologies evolve, the criminalization of the technique used to create *"deep fakes"* is not efficient, but rather of their criminal results. Thus, the most appropriate solution would be the creation of a qualifier or cause for increasing the penalty for crimes committed through this practice, to discourage the practice of such offense.

The focus of this research was the search for a way to combat the spread of harmful *"deep fakes"* through state punishment. Thus, it is limited in the sense that it does not comprehensively explore the moral and ethical implications of the practice of "*deep fakes",* such as the question of the individual's consent and their right to privacy and image, as well as in seeking alternative and preventive solutions to help combat "*deep fakes".* Thus, research is needed that encompasses such themes in detail, in order to contribute to the social and legal advancement of society.

REFERENCES

1. Aires, R. W. do A., Moreira, F. K., & Freire, P. de S. (2017). Indústria 4.0: competências requeridas aos profissionais da quarta revolução industrial. *Anais do VII Congresso Internacional de Conhecimento e Inovação, 1*(1). Disponível em: <https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/314>. Acesso em: 30 abr. 2024.

2. Após atingir pico de óbitos, Brasil tem queda de 90% na média diária de mortes por covid-19. (2021). *GZH SAÚDE*. Disponível em: <https://gauchazh.clicrbs.com.br/saude/noticia/2021/10/apos-atingir-pico-de-obitos-brasil-tem-queda-de-90-na-media-diaria-de-mortes-por-covid-19-ckuxys2ts0007017fzwxl3u0e.html>. Acesso em: 30 abr. 2024.

3. Brasil. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Rio de Janeiro, RJ: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 20 abr. 2024.

4. Brasil. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Rio de Janeiro, RJ: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm>. Acesso em: 20 abr. 2024.

5. Brasil. Decreto-Lei nº 4.657, de 4 de setembro de 1942. Lei de Introdução às normas do Direito Brasileiro. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm>. Acesso em: 20 abr. 2024.

6. Brasil. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 21 abr. 2024.

7. Brasil. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21 abr. 2024.

8. Brasil. Projeto de Lei do Senado Federal nº 473 de 2017. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar o crime de divulgação de notícia falsa. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/131758>. Acesso em: 20 abr. 2024.

9. Câmara dos Deputados. CPI – Crimes Cibernéticos. Brasília: [s. n.], 2016. 254 p. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPI CIBER+%3D%3E+RCP+10/2015>. Acesso em: 30 abr. 2024.

10. Capez, F. (2011). *Curso de Direito Penal: Parte Geral* (15. ed.). São Paulo: Saraiva.

11. Da Costa, F. J. (2011). *Locus delicti nos crimes informáticos* (Tese de Doutorado). Faculdade de Direito, Universidade de São Paulo, São Paulo. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php>. Acesso em: 30 abr. 2024.

12. Estevão, R. da F., & Brito Filho, C. M. (n.d.). Princípio da proibição da proteção deficiente: função

e missão do Direito Penal. In: Revista da AJURIS - Associação dos Juízes do Rio Grande.

13. Faustino, A. (2018). *Fake news e a liberdade de expressão nas redes sociais na sociedade da informação* (Dissertação de Mestrado). Faculdades Metropolitanas Unidas, São Paulo. Disponível em: <http://arquivo.fmu.br/prodisc/mestradodir/af.pdf>. Acesso em: 25 abr. 2024.

14. Furbino, C. S., & Souza, T. I. de. (2021). Fake news contribuindo para o cibercrime: regulação e necessidade de tipificação atreladas à legislações internacionais. In *XII Congresso RECAJ - UFMG Skema Business*, Belo Horizonte, 44-50. Disponível em: <http://site.conpedi.org.br/publicacoes/f0d20hl5/k6f200vz>. Acesso em: 25 abr. 2024.

15. Greco, R. (2017). *Curso de Direito Penal: Parte Geral* (19.ed.). Niterói: Impetus. ISBN 978-85-7626-930-4.

16. Grigori, P. (2018, maio 11). 20 projetos de lei no Congresso pretendem criminalizar fake news. Disponível em: <https://apublica.org/2018/05/20-projetos-de-lei-no-congresso-pretendem-criminalizar-fake-news/>. Acesso em: 24 abr. 2024.

17. Harari, Y. N. (2024). *Sapiens: uma breve história da humanidade*. Porto Alegre: L&PM Editores.

18. Jesus, D. de, & Milagre, J. A. (2016). *Manual de Crimes Informáticos*. São Paulo: Saraiva. ISBN 978850262724-6.

19. Lacerda, A. C. A. M. de, & Silva, A. P. (2021). Cibercrime: evolução do crime e a banalização dos crimes virtuais. In F. H. da S. Horita, F. S. de Morais, & C. M. de Oliveira (Orgs.), *Direito Penal e Cibercrimes* (1 ed., v. 1, pp. 12-19). Belo Horizonte: Skema Business School.

20. Lima Filho, P. R. A. de. (2021). O Direito Penal na Quarta Revolução Industrial. *Delictae Revista De Estudos Interdisciplinares Sobre O Delito, 6*(10), 215-304. Disponível em: <https://doi.org/10.24861/25265180.v6i10.150>. Acesso em: 30 abr. 2024.

21. Maues, G. B. K., Duarte, K. C., & Cardoso, W. R. da S. (2018). Crimes virtuais: uma análise sobre a adequação da legislação penal brasileira. *RIOS Eletrônica (FASETE, 18*, 166-180). Disponível em: <https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf>. Acesso em: 30 abr. 2024.

22. Medon, F. (2021). O direito à imagem na era das deepfakes. *Revista Brasileira de Direito Civil – RBD Civil: Belo Horizonte, 27*, 251-277. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/viewFile/438/447>. Acesso em: 30 abr. 2024.

23. Piaia, T. C., Costa, B. S., & Willers, M. M. (2019). Quarta revolução industrial e a proteção do indivíduo na sociedade digital: desafios para o direito. *Revista Paradigma, 28*, 122-140. Disponível em: <https://revistas.unaerp.br/paradigma/article/view/1444/1287>. Acesso em: 25 abr. 2024.

24. Pinheiro, P. P. (2021). *Direito Digital* (7. ed.). São Paulo: Saraiva Educação. 573 p. ISBN 9786555598438.

25. Rudolfo, F. M. (2011). *A dupla face dos direitos fundamentais: a aplicação dos princípios da proibição de proteção deficiente e de excesso de proibição no direito penal, especialmente quanto aos crimes sexuais* (Dissertação de Mestrado). Universidade Federal de Santa Catarina,

Florianópolis, SC. Disponível em: <https://repositorio.ufsc.br/xmlui/handle/123456789/95755>. Acesso em: 25 abr. 2024.

26. Santos, M. F. P. dos. (2015). *Retórica, teoria da argumentação e pathos: o problema das emoções no discurso jurídico* (Dissertação de Mestrado). Universidade de Brasília, Brasília. Disponível em: <https://repositorio.unb.br/handle/10482/18787#:~:text=Este%20estudo%20objetiva%20compreender%20por,a%20explana%C3%A7%C3%A3o%20do%20sistema%20jur%C3%ADdico>. Acesso em: 25 abr. 2024.

27. Schwab, K. (2016). *A Quarta Revolução Industrial*. São Paulo: Edipro. ISBN 978-85-7283-978-5.

28. Terra, C. I. de S., Orsini, A. G. de S., & Abreu, C. C. de M. (2021). Crimes cibernéticos: phishing e fake news em tempos de pandemia. In S. H. Z. Freitas, Y. N. da C. Lannes, & L. J. R. da Silva (Orgs.), *Criminologia e cybercrimes* (pp. 29-35). Belo Horizonte: UFMG. Disponível em: <http://site.conpedi.org.br/publicacoes/f0d20hl5/k6f200vz>. Acesso em: 26 abr. 2024.

29. Wakefield, J. (2022, março 18). Guerra na Ucrânia: os ‘presidentes deepfake’ usados na propaganda do conflito. *BBC News*, São Paulo, SP. Disponível em: <https://www.bbc.com/portuguese/internacional-60791955>. Acesso em: 26 abr. 2024.

30. Waldman, R. L., & Horas, M. dos S. (2018). Uma caracterização das fake news: o exemplo da greve dos caminhoneiros. In *Direito, governança e novas tecnologias I* (pp. 338-353). CONPEDI/UNISINOS, Florianópolis. Disponível em: <http://site.conpedi.org.br/publicacoes/34q12098/9l053031>. Acesso em: 26 abr. 2024.