


## DEEPPAKES AND PRIVACY PROTECTION: THE PARADOX BETWEEN PRIVACY AND ARTIFICIAL INTELLIGENCE

 <https://doi.org/10.56238/arev6n4-103>

Submitted on: 09/11/2024

Publication date: 09/12/2024

**Izabela Alves Drumond Fernandes<sup>1</sup>**

---

### ABSTRACT

INTRODUCTION: Society has been constantly transformed, especially with regard to Artificial Intelligence (AI) and its use by society. It has arrived to revolutionize the lives of everyone who has access to it, boosting several areas and forms of interaction. However, this advance brings with it some conflicts that need to be resolved.

The inclusion of AI in Brazil is relatively new. According to data from the Getúlio Vargas Foundation, in 2022 there were 64 judicial Artificial Intelligence projects being developed for the application of artificial intelligence in the judiciary.

**Keywords:** Deepfakes. Privacy. Artificial intelligence. Data Protection.

---

<sup>1</sup> State University of Montes Claros (UNIMONTES) – Minas Gerais  
E-mail: izabeladrumond@hotmail.com

## INTRODUCTION

Society has been constantly transformed, especially with regard to Artificial Intelligence (AI) and its use by society. It has arrived to revolutionize the lives of everyone who has access to it, boosting several areas and forms of interaction. However, this advance brings with it some conflicts that need to be resolved.

The inclusion of AI in Brazil is relatively new. According to data from the Getúlio Vargas Foundation, in 2022 there were 64 judicial Artificial Intelligence projects being developed for the application of artificial intelligence in the judiciary.

In this regard, with the disorderly growth of AI arises the need to regulate privacy ensuring respect for it as a fundamental right and for this the following question arises: Is AI preserving the fundamental right to privacy of its users through *deepfakes*?

The main objective will be to analyze whether the innovation brought by AI meets the preservation of the privacy of its users, seeking to demonstrate possible solutions that can reconcile technological innovation and the preservation of the fundamental right.

It is verified that, on the one hand, there is AI that depends on the collection and analysis of personal data to work efficiently and provide the expected benefits and, on the other hand, this access threatens the privacy of its users, exposing them to risks such as algorithmic discrimination and the misuse of personal information.

To this end, it is observed that AI has brought some challenges to human rights, especially with regard to the protection of the privacy of its users.

The right to privacy is enshrined in the UDHR, by the General Data Protection Regulation (GDPR) of the European Union, as well as by article 5, X, XI and XII of the CRFB, which provides for the right to privacy as a fundamental right that must be safeguarded by all.

In addition to the respective normative instruments, there is the General Law for the Protection of Personal Data (Law 13.709/2018) which aims to protect sensitive personal data, having respect for privacy as one of the foundations.

In this sense, as AI evolves, the challenges increase every day because, through AI, algorithms are able to process an alarming volume of data, which will imply the violation of privacy and data security, thus generating a paradox between technology and the protection of the fundamental right to privacy.

Faced with this impasse, PL 2338/2023 emerges, which provides for the use of artificial intelligence and the regulation of privacy within AI in order to protect fundamental rights.

The work will be divided into three sections, the first of which will discuss privacy, its concept and the interconnection with fundamental rights. In the second section, fundamental rights were addressed, especially with regard to privacy. In the second section, the technological evolution of artificial intelligence, how it came about and the existing protection mechanisms, and finally, in the third section, *deepfakes* and digital reconstruction were discussed, demonstrating the paradox between privacy and technological evolution.

For the elaboration of the work, the qualitative approach method will be used, interpreting the technological innovations and their impact on the privacy of its users. The method of procedure will be bibliographic through the literature review on AI as well as the protection of privacy and the use of the algorithms used by it. The data collection technique will be done through articles, reports, and studies that address AI and privacy.

## **PRIVACY AND FUNDAMENTAL RIGHTS**

Privacy is a fundamental right, essential for the preservation of human dignity and, when analyzing privacy from a historical point of view, it refers to capitalism that has undergone changes in the concept of private life. The decline in privacy was due to the use of new technologies that exposed private life to society (Thibes, 2017).

Privacy did not exist in the past, it is the result of personal feelings and convictions, which do not harm society and are considered the freedoms that each person has

the concept of the right to privacy implies a freedom legally recognized to each individual, who must be free not only as a citizen with rights, and as a subject of law governed by laws, but as a person with a distinct space in relation to society, which is safeguarded from a state and legal point of view, both nationally and internationally (Correia, 2014, p. 13).

In this sense, it is verified that the individual needs to have his rights respected and the law needs to ensure that these will not be violated.

According to Warren; Brandeis, (1890, p. 196) "some inventions and business models then emerging, such as photography and the journalistic enterprise, were exposing people's intimacy and, consequently, their privacy". In this sense, the authors began to discuss the creation of a law that could ensure the privacy of the individual, considering

that the damage caused by these invasions of privacy could cause immeasurable suffering. To this end, it was necessary that the exposure occurred with the individual's consent, that is, "the right to privacy ceases with the publication of the facts by the individual or with his consent" (Warren; Brandeis, 1890, p. 218).

With this, it is observed that, over the years, international documents for the protection of the private life and intimacy of the individual have been approved. The first document to address privacy in an implicit way was the American Declaration of the Rights and Duties of Man, in 1948, through its Article I. "Everyone has the right to life, liberty and security of his person".

Parallel to it, with the creation of the Organization of American States (OAS) in 1948, the rights inherent to the individual as well as his duties should be ensured and enforced.

In the same year, the UN General Assembly approved the Universal Declaration of Human Rights (UDHR), which aims to promote respect for individual rights and freedoms at the national and international levels, and this protection needs to be safeguarded by Member States.

In 1950, through the European Convention for the Protection of Human Rights and Fundamental Freedoms, it guaranteed the development of fundamental rights and freedoms.

In 1966, the UN General Assembly approved the International Covenant on Civil and Political Rights, in force since 1976,<sup>2</sup> reaffirming the UDHR, considering that at that time the binding force of the UDHR was being discussed and with that, it would need a document that would bind the Member States to make it effective. (Piovesan, 2016).

The Pact of San José, Costa Rica, adopted in 1969 and ratified by the OAS Member States, was established to ensure the protection of and respect for human rights by the signatory states. In the event of a violation of these rights, after exhaustion of domestic legal remedies, the injured individual or group may file a complaint with the Inter-American Commission on Human Rights. If the situation remains unresolved, the Commission has the prerogative to refer the case to the Inter-American Court of Human Rights, which is responsible for judging and determining the necessary measures.

In 2000, the European Union signed the Charter of Fundamental Rights, which aims to strengthen and protect the fundamental rights, freedoms and principles of society, as

---

<sup>2</sup> The present Covenant took a little longer to enter into force as it did not have the number of ratifications necessary to make it applicable.

stated in article 7: "Respect for private and family life. Everyone has the right to respect for their private and family life, their home and their communications".

In view of the documents presented, it can be seen that the evolution of the right to privacy was foreseen as a fundamental right and should be put into effect by the Member States.

It can be seen that the respective instruments serve to protect the privacy of that individual, however, even though it is a fundamental right, it becomes complex when the information is of public interest. "It is difficult to qualify [an action] as a violation of the right to privacy when there is a reasonable justification, a legitimate purpose, or even implicit consent of the person whose privacy was intruded" (Correia, 2014).

In this sense, the right to privacy cannot be considered an absolute right, and it is necessary to balance the right to information with privacy, considering that it is a right that belongs to all people and that allows no one to interfere with their intimacy or privacy.

The CRFB establishes in its article 5, item X, the inviolability of "intimacy, private life, honor and image of persons, ensuring the right to compensation for material or moral damage resulting from its violation" (Brasil, 1988).

The Civil Code of 2002, on the other hand, protects the rights of personality related to honor and image in its article 11<sup>3</sup>. Article 20<sup>4</sup> prohibits the exposure or use of someone's image without permission.

The Penal Code typifies the crimes of slander, defamation and slander in articles 139 to 140, and slander would be imputing a criminal fact to someone. Defamation would be to point out a fact offensive to someone's reputation and, finally, injury would be to offend the dignity or decorum of a certain person.

On April 23, 2014, Law No. 12,965 was published, which establishes principles, guarantees, rights and duties for the use of the Internet in Brazil, being considered the Civil Rights Framework for the Internet. It does not necessarily deal with privacy, being one of the most advanced normative instruments on internet regulation, according to the 2016 CPI Report on Cybercrimes. The Law established the guarantee of privacy, freedom of expression, intimacy of users, prohibition of disclosure of personal data, among others.

---

<sup>3</sup> Article 11. Except in the cases provided for by law, personality rights are non-transferable and non-waivable, and their exercise cannot be voluntarily limited.

<sup>4</sup> Article 20. Unless authorized, or if necessary for the administration of justice or the maintenance of public order, the dissemination of writings, the transmission of the word, or the publication, exhibition or use of the image of a person may be prohibited, at his request and without prejudice to the compensation that may be due, if it affects his honor, good reputation or respectability, or if they are intended for commercial purposes

The respective Law establishes the protection of privacy in articles 3, 7, 8, 10, 11:

Art. 3 The discipline of the use of the Internet in Brazil has the following principles:  
[...]

II - protection of privacy;

[...]

Art. 7 Access to the Internet is essential to the exercise of citizenship, and the user is guaranteed the following rights:

I - inviolability of intimacy and private life, its protection and compensation for material or moral damage resulting from its violation;

[...]

Article 8 The guarantee of the right to privacy and freedom of expression in communications is a condition for the full exercise of the right to access the Internet. Sole Paragraph. Contractual clauses that violate the provisions of the caput, such as those that:

I - imply offense to the inviolability and secrecy of private communications, over the internet; or

II - in an adhesion contract, do not offer as an alternative to the contracting party the adoption of the Brazilian forum for the resolution of disputes arising from services rendered in Brazil.

[...]

Article 11. In any operation of collection, storage, custody and treatment of records, personal data or communications by connection providers and internet applications in which at least one of these acts occurs in the national territory, Brazilian legislation and the rights to privacy, protection of personal data and confidentiality of private communications and records must be compulsorily respected.

It should be noted that it must protect users as well as clarify the protection of personal data, private communications, connection records and access to internet applications must preserve the intimacy, private life, honor and image of the parties directly or indirectly involved and, if they are not protected, will incur the sanctions provided for in article 12<sup>5</sup> which ranges from a warning, a fine of up to 10% of the economic group's revenue in Brazil in its last fiscal year, temporary suspension of activities and even prohibition from exercising the offender's activities.

---

<sup>5</sup> Article 12. Without prejudice to other civil, criminal or administrative sanctions, violations of the rules provided for in arts. 10 and 11 are subject, as the case may be, to the following sanctions, applied separately or cumulatively:

I - warning, with indication of the deadline for the adoption of corrective measures;

II - a fine of up to 10% (ten percent) of the economic group's revenues in Brazil in its last fiscal year, excluding taxes, considering the economic condition of the offender and the principle of proportionality between the seriousness of the offense and the intensity of the sanction;

III - temporary suspension of activities involving the acts provided for in article 11; or

IV - prohibition of the exercise of activities involving the acts provided for in article 11.

Sole Paragraph. In the case of a foreign company, its branch, office or establishment located in the country is jointly and severally liable for the payment of the fine referred to in the caput.

In 2018, inspired by the European Union's General Data Protection Regulation (GDPR),<sup>6</sup> Brazil enacts Law 13,709, entitled General Data Protection Law (LGPD), which regulates the processing of personal data protection that provides in its article 1:

Article 1: On the processing of personal data, including in digital media, by an individual or by a legal entity governed by public or private law, with the objective of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person.

The respective Law does not specifically address *deepfakes*<sup>7</sup>, but provides an overview that can be used to protect personal data involving the use of AI. It brought in its articles 5, 7, 18, 46, 52 and 54 some terms such as: personal, sensitive and anonymized data, database, holder, processing, consent and international transfer, among others. It also determines that, only upon the provision of written consent by the data owner is the processing of personal data allowed, which can be revoked at any time if the latter disagrees with any change in the purpose of the data processing; for compliance with a legal or regulatory obligation by the controller.

## **HISTORICAL EVOLUTION OF ARTIFICIAL TECHNOLOGICAL INNOVATION**

AI went through several modernization processes until it personified *online services* in order to improve and provide practicality to its users, however, this process was marked by a complex trajectory of technological advances and changes, from the origin of the computer to the present day.

Before addressing the historical evolution of AI, it is necessary to know its disruptive character<sup>8</sup>, which presents itself with technologies capable of innovating and bringing significant changes in people's lives, changing their lifestyle habits. In this way, it is

---

<sup>6</sup> The General Data Protection Regulation (GDPR) came into effect on May 25, 2018, replacing the 1995 EU Data Protection Directive. On January 1, 2021, the approved version of the European Union GDPR law went into effect in the United Kingdom (UK GDPR). It served as a guideline for the publication of Law 13.709/2018.

<sup>7</sup> Deepfake means "deep falsehoods" that "became popular from the story of a user of the Reddit website, who nicknamed himself Deepfake and, specializing in artificial intelligence, began to replace people's faces in movies. 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 one notice that it is a montage". Available at: [http:// www.cienciadigital.com.br/2018/06/06/deepfake-era-digital-e-o-fim-do-direito-imagem/](http://www.cienciadigital.com.br/2018/06/06/deepfake-era-digital-e-o-fim-do-direito-imagem/). Accessed on: 1 nov. 2024.

<sup>8</sup> The term was coined by Clayton Christensen and Joseph Bower in the article Disruptive Technologics: catching the wave, published in 1995 by the Harvard Business Review. The initial concept of disruptive innovation is closely linked to the effect of disruptive technologies on the market as a value proposition differentiated from that previously available.



possible to say that AI has this disruptive character since it has arrived to revolutionize the lives of its users with simplicity and economy. (Christensen et al., 2015).

In 1943, "AI was first mentioned in an article written by writers Warren McCulloch and Walter Pitts who discussed artificial forms of reasoning using the mathematical model mimicking the human nervous system."<sup>9</sup> This model emerged as a basis for academic questions on the subject.

In the twentieth century, they began to develop the first theoretical foundations of AI, through the creation of computing, with Alan Turing being one of the pioneers in this process. He proposed, in his article, "Computing Machinery and Intelligence" (1950), a way to test the machine's ability to exhibit human behavior, launching the later debates on AI (Turing, 1950).

It was found that among the experiences of the war, the concentration camps made it possible for the Nazis to carry out research and experiments with the brain and human intelligence, being developed against human dignity, which is unacceptable.

The beginning of AI effectively took place in 1956 at the Dartmouth College Conference, in New Hampshire (USA), in which the terminology "artificial intelligence" used to express the new field of knowledge was recorded for the first time (Russell; Norvig, 2009). At this event, the researchers believed that, in a short time, machines could reach human intelligence.

It turns out that the complexity in development as well as the lack of investments were key factors for the stagnation of research. In this sense, Minsky (1967) points out that: "no one could have foreseen how difficult it would be to make the machines that think". In other words, they began to realize that there would be many technological limitations and what would be brief would take years to be realized.

AI appeared approximately in the century. with the displacement of the center of power through the humanist revolution, starting to use non-human algorithms<sup>10</sup> (Harari, 2016, p. 347).

In addition to power, AI faces problems in security and in the fact that it does not know how the control of machines would be done and how it would act in the future. For Harari (2016), if the expectations around AI are confirmed in the coming years, we will have

<sup>9</sup> Available at: <https://www.institutodeengenharia.org.br/site/2018/10/29/a-historia-da-inteligencia-artificial/#:~:text=Em%201943%2C%20Warren%20McCulloch%20e,IA%20capaz%20de%20jogar%20xadrez.>

<sup>10</sup> The algorithm is a finite sequence of actions that solves a certain problem that can solve different problems.



a radical shift in the center of power: "The new technologies of the twenty-first century can thus reverse the humanist revolution, depriving humans of their authority and passing power to non-human algorithms" (Harari, 2016, p. 347).

In 1990, Yann LeCun brought the explanation through which: "the reason why AI has progressed so rapidly in recent years is the availability of large amounts of data and the exponential increase in computational power" (LeCun, 2015), that is, for him, it was not working because the algorithms had not been boosted, and it was possible to verify through *deep learning*<sup>11</sup> that it brought more effective approaches.

In the face of advances, companies such as Facebook, Google, and Tesla began to invest in AI, revolutionizing the new technological era.

Initially, AI was developed to solve complex problems and improve access for its users. Today it has been increasingly used as a tool of social control. AI systems are able to analyze data, understand behaviors, and define future actions, which gives them full control over the lives of their users. Through this control by AI, concerns arise about the privacy of its users.

## **DEEPFAKES AND DIGITAL RECONSTRUCTION: THE PARADOX BETWEEN PRIVACY AND TECHNOLOGICAL EVOLUTION**

With the advancement of technology, it is increasingly easy to create untrue videos and images of situations that never happened and consequently, privacy is increasingly threatened. This digital forgery is being used to propagate *fake news*, impersonate celebrities, manipulate elections and apply scams, both with the image and voice of a certain person.

It appears that the use of surveillance technologies, through biometrics<sup>12</sup>, facial recognition, data collection through social networks are examples of how AI can invade the private waiting of its user without their consent. This disorderly use of data not only hurts privacy but also the indiscriminate use of data.

According to the National Data Protection Authority (ANPD) (2024, p. 11):

<sup>11</sup> The term "deep learning" emerged in the 1980s with the work of computer scientist Geoffrey Hinton. He conducted studies on neural networks, creating a model known as a "deep neural network," which relies on the structure of the human brain for data processing. This area emerged with the studies on artificial neural networks in the 40s. Available at: Unraveling the Mysteries of Deep Learning: A Journey through Cutting-Edge Artificial Intelligence (andrelug.com)

<sup>12</sup> The biometric technologies used in facial recognition can be used for various purposes, starting from simple presence detection to more complex levels such as identification, verification, and classification of individuals (EPRS, 2021b).

Nevertheless, in contrast to the new possibilities that the use of biometrics can provide, significant concerns arise about the privacy and protection of the personal data of data subjects, especially in relation to facial recognition and its growing use in Brazil and worldwide.

Through this facial recognition, the false use of images generated by AI is known as *deepfake*, a term derived from *Deep Learning*, and *Fake*, referring to the generation of content by artificial neural networks (Mirsky; Lee, 2021). The tampering of users' images is increasingly frequent, whether through images or through voice, creating fictitious content (Zhang et al., 2021).

The social impacts are increasingly devastating, with legal implications, with the violation of image, identity, privacy, and intellectual property, resulting in economic and moral losses for users.

It turns out that the forgeries are not noticeable, which makes it more complex to demonstrate tampering. Faced with this difficulty, companies are looking for effective solutions through Meta and some universities support to be able to curb these forgeries and adulterations.

In Brazil, there is still no specific legislation on the monitoring of facial recognition, however, there are bills in progress in Congress that address this issue and how to use it, namely: PL No. 3,069/2022 (public security); PL nº. 3,822/2023 (financial system); PL nº. 12/2015 (civil area) and the standardization of PL No. 2,338/2023 (artificial intelligence).

In the current scenario, if any deepfake is proven, this case may be reported to the ANPD, which will require the removal of the content. In more serious cases, the person who has their image violated may request compensation for moral damages through legal action.

## PRESERVING PRIVACY IN THE FACE OF TECHNOLOGICAL INNOVATION

Artificial Intelligence (AI) has transformed various aspects of modern life, from the economy to health, including entertainment and communication. However, one of its most controversial applications is the use of AI as a tool for social control. This article explores how AI can be used to monitor, influence, and constrain behaviors in contemporary societies, addressing the ethical implications and challenges associated with this phenomenon. Also discussed are the impacts of mass surveillance, the manipulation of public opinion, and restrictions on individual freedom, as well as the urgent need for regulation and ethical oversight of these technologies.

AI emerged to make life easier for its users and, with the advancement of technology, the digital world has incorporated people's lives, impacting social processes and structures.

Mass surveillance is one of the most used forms by AI in social control. Cameras with facial recognition, sensor networks, and data analysis systems allow the government and companies to monitor the collective and individual activities of their users.

It is worth mentioning that, when AI is used consciously, it has achieved benefits through data processing, as Santiso (2022, p.77) adds:

With regard to the use of AI, the potential contribution to the achievement of social and economic benefits is highlighted with advances, among other aspects, in the provision of services by governments. This technology offers the possibility of making these services more efficient, equitable and personalized. However, while there is no doubt about the opportunities and potentialities it offers, its development and implementation also entail multiple challenges for society, starting with the risk of discrimination against groups and individuals, the misuse of data or the violation of the right to privacy<sup>13</sup>.

In this sense, AI improves government services and promotes social and economic advances, that is, it offers the benefits it promises, can access a large number of data, in the case of the use of public security systems, use smart cameras, and facial recognition increases security and inhibits the practice of crimes (Santos, 2024).

It is observed that technological innovation, especially the accelerated development of (AI), has profoundly transformed society, driving advances in several areas, such as health, safety, economy, and even in the way we communicate and interact.

In China, for example, AI can be used to assess citizens' behavior by collecting data on daily activities, such as shopping and social interactions, assigning scores that will influence people's lives (Pohlmann, 2019).

AI is being used to determine behaviors, representing a new form of power through which individual freedoms are subordinated to the interests of those who control the technology.

---

<sup>13</sup> Emerging technologies, and in particular artificial intelligence (AI), have a high disruptive potential to restore public administrations in the digital age, improving public policy-making, service delivery to citizens, and the internal efficiency of administrations. The public sector can increase its ability to achieve social, economic, and environmental impacts for the well-being of citizens, as long as AI is implemented ethically and strategically. (Author's translation)

In addition, there is also the use of algorithms that are used by social media platforms in order to filter content and direct advertising to users, even to the point of manipulating emotions.

## THE VIOLATION OF PRIVACY IN THE FACE OF TECHNOLOGICAL INNOVATION

AI can be used to limit its user's individual freedom of choice by diverting their own interests to the interests manipulated by it. Nowadays, if someone talks about a certain subject, close to the cell phone it will send you to all possible research on the subject you had talked about, given this, you can see the constant monitoring of networks in the lives of their users and the way they are manipulated.

It is observed that the use of bots and deepfakes has been used to propagate false information and polarize societies. In this sense, Rivelli (2024, n.n.) establishes that: "in the first nine months of 2023 alone, about 240 thousand deepfake videos were uploaded to the 35 main pornography sites in the world".

It can be seen that the spread and impact of *deepfake* technologies, especially in the context of pornography, is rapid. It is observed that the numbers are alarming and reveal a dynamic in which advanced artificial intelligence tools are being used to create falsified content, often without the consent of users, which raises social, ethical and legal issues.

This time, it is urgent to regulate the use of technology, even if it is at the service of the population that uses it, that is, it is necessary to have regulation for such use. In this sense, it can be seen that in other countries there are already specific laws that criminalize *deepfakes* for malicious purposes, as is the case in some North American states, such as California, New York, Texas and Virginia, and in countries such as Australia, South Africa and Great Britain. "The MyImage MyChose Foundation demonstrated that abusive deepfakes went from the level of 144 thousand in 2019 to 270 thousand this year, growing 1,780% and viewed 4 billion times" (Riveli, 2024, s.n.).

The agent responsible for data processing, provided for in the LGPD, must foresee the dangers that data subjects will be exposed to, in addition to structuring the systems in order to meet the security requirements and principles provided for in the LGPD, as recommended by article 49 of the respective law:

Article 49: The systems used for the processing of personal data must be structured in such a way as to meet the security requirements, the standards of good practices

and governance, and the general principles provided for in this Law and other regulatory standards.

If, on the one hand, there is an evolution in the technological plan, on the other hand, there is a setback and a real violation of the privacy of its users through the leakage of biometric data, identity, which generates emotional wear and tear that no indemnity can pay, in addition, what falls on the internet no longer disappears.

It is observed that, even though Brazil does not have its own regulation, there are several bills on the subject, in the scope of criminal law there is PL No. 1272/2023 that amends Decree-Law No. 2,848/1940 (Penal Code), to create the crime of article 308-A – malicious tampering of videos or audios; PL 623/2024 that amends Decree-Law No. 2,848/1940 (Penal Code), to typify the crime of image manipulation in an unauthorized manner and Bill No. 146/2024 that amends Decree-Law No. 2,848/1940 (Penal Code), to establish a cause for increasing the penalty for crimes against honor and a qualified hypothesis for the crime of false identity, for when artificial intelligence technology is used to alter the image of a person or human sound.

In the field of the Consumer Protection Code (CDC), there is PL No. 145/2024, which amends Law No. 8,078, of September 11, 1990 (Consumer Protection Code), to regulate the use of artificial intelligence tools for advertising purposes and curb misleading advertising with the use of these tools.

In addition to these, the Federal Council of the OAB approved, on November 11, 2024, a series of recommendations to guide the use of generative artificial intelligence in legal practice. This recommendation aims to establish guidelines that promote ethics and responsibility in the use of these technologies, aiming to ensure that the use of AI in law is aligned with the fundamental principles of the profession and legal requirements.

## **FINAL CONSIDERATIONS**

AI has changed people's lives, having great potential to offer immeasurable benefits, it turns out that the balance between innovation and privacy protection is one of the great challenges in current times.

In order to have legal certainty for its users, it is not only necessary to regulate, but also to monitor and implement laws, in addition to reinforcing laws that protect the privacy of individuals, LGPD, which establish clear standards for the collection and use of personal data.

In addition, it is necessary that in this implementation education about human rights, privacy and the risks of AI be promoted both in the lives of its users and the general public.

It is observed that the problems arising from the use of *deepfakes* have worried their users, in view of this, several proposals for Bills have emerged in order to regulate the use of technology related to *deepfakes*.

However, only with effective and effective regulation will it be possible to keep up with technological advances without users being afraid of having their dignity violated, that is, it is essential to balance the benefits of AI with the adoption of public policies and practices that guarantee the protection of fundamental rights, such as privacy, equality, and transparency.

## REFERENCES

1. A história da inteligência artificial. (2018, outubro 29). Instituto de Engenharia. Disponível em: <https://www.institutodeengenharia.org.br/site/2018/10/29/a-historia-da-inteligencia-artificial/#:~:text=Em%201943%2C%20Warren%20McCulloch%20e,IA%20capaz%20de%20jogar%20xadrez>. Acesso em: 20 nov. 2024.
2. Cebrian, F. S. P. F., et al. (2024). Biometria e reconhecimento facial: estudos preliminares. ANPD. Brasília, DF. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/radar-tecnologico-biometria-anpd-1.pdf>. Acesso em: 15 nov. 2024.
3. Bittar, C. A. (2015). Os direitos da personalidade (8ª ed.). São Paulo: Saraiva.
4. Brandeis, L. D., & Warren, S. D. (2024). O direito à privacidade. Revista de Direito Civil Contemporâneo, 38, 391-417.
5. Brasil. (1988). Constituição da República Federativa do Brasil. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 10 nov. 2024.
6. Brasil. (1992). Decreto No 592, de 6 de julho de 1992. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/decreto/1990-1994/d0592.htm](https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm). Acesso em: 20 nov. 2024.
7. Brasil. (2014). Lei Nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 09 nov. 2024.
8. Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Diário Oficial da União, Brasília. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 12 nov. 2024.
9. Deepfake: A era digital e o fim do direito à imagem. (2018, junho 6). Ciência Digital. Disponível em: <http://www.cienciadigital.com.br/2018/06/06/deepfake-era-digital-e-o-fim-do-direito-imagem/>. Acesso em: 1 nov. 2024.
10. Rivelli, F. (2024). Combatendo deepfakes: Desafios de gênero na regulação contra a violência digital. Disponível em: <https://www.migalhas.com.br/coluna/ia-em-movimento/405037/combateendo-deepfakes>. Acesso em: 15 nov. 2024.
11. Filho, G. (2023). Inteligência artificial e aprendizagem de máquina: aspectos teóricos e aplicações. São Paulo: Blucher.



12. Medon, F. (2021). O direito à imagem na era das deepfakes. Disponível em: [file:///C:/Users/izabe/Downloads/438-Texto%20do%20Artigo-2189-2082-10-20210409%20\(3\).pdf](file:///C:/Users/izabe/Downloads/438-Texto%20do%20Artigo-2189-2082-10-20210409%20(3).pdf). Acesso em: 22 nov. 2024.
13. Minsky, M. (2003). Semantic Information Processing. Cambridge: MIT Press.
14. Mirsky, Y., & Lee, W. (2020). The Creation and Detection of Deepfakes: A Survey. Disponível em: <https://arxiv.org/abs/2004.11138>. Acesso em: 18 nov. 2024.
15. Moraes, T. G., et al. (2024). Biometria e reconhecimento facial. ANPD. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/radar-tecnologico-biometria-anpd-1.pdf>. Acesso em: 15 nov. 2024.
16. Organização das Nações Unidas (ONU). (1948). Declaração Universal dos Direitos Humanos da ONU. Disponível em: <https://www.oas.org/dil/port/1948%20Declara%C3%A7%C3%A3o%20Universal%20dos%20Direitos%20Humanos.pdf>. Acesso em: 20 nov. 2024.
17. ONU. (1966). Pacto Internacional dos Direitos Econômicos, Sociais e Culturais. Disponível em: <https://www.oas.org/dil/port/1966%20Pacto%20Internacional%20sobre%20os%20Direitos%20Econ%C3%B3micos,%20Sociais%20e%20Culturais.pdf>. Acesso em: 15 nov. 2024.
18. OEA. (1969). Convenção Americana de Direitos Humanos (“Pacto de San José de Costa Rica”). Disponível em: <https://www.oas.org/juridico/portuguese/treaties/b-32.htm>. Acesso em: 10 nov. 2024.
19. Piovesan, F. (2016). Temas de direitos humanos. São Paulo: Saraiva.
20. Pohlmann, M. (2024). George Orwell na China: digitalização como meio de controle social total. Disponível em: <https://www.jota.info/artigos/george-orwell-na-china-digitalizacao-como-meio-de-controle-social-total>. Acesso em: 22 nov. 2024.
21. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. (2016, abril 27). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 10 nov. 2024.
22. Rodotà, S. (2008). A vida na sociedade da vigilância – A privacidade hoje. Rio de Janeiro: Renovar.
23. Santiso, C., Flores, C., & Mejía Jar Amillo, M. I. (2024). Conceptos fundamentales y uso responsable de la inteligencia artificial em el sector público. Disponível em: <https://scioteca.caf.com/bitstream/handle/123456789/1921/Conceptos%20fundamentales%20y%20uso%20responsable%20de%20la%20inteligencia%20artificial%20en%20el%20sector%20p%C3%BAblico.pdfsequence=5&isAllowed=y>. Acesso em: 10 out. 2024.

24. Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, 59(236), 433-460. Disponível em: [ARACÊ MAGAZINE, São José dos Pinhais, v.6, n.4, p.12659-12674, 2024](https://watermark.silverchair.com/lix-236-433.pdf?token=AQECAHi208BE49Ooan9kKhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAA A10wggNZBgkqhkiG9w0BBwagggNKMIIDRglBADCCAz8GCSqGSIlb3DQEHATAeB glghkgBZQMEAS4wEQQMTUu5BpFAV-m3JniwAgEQglIDEGsHo59fZyjgtgTUw30AxWcAXW4lQ-Teatc5mDw1fc9O5lZX-_8krxpDIEerLcTa61XIR2lgeSFf2whRUMPqj00QuOmlGDfaftx8q4z-BK15oxHVptlO4TG9yQt9GyngFD1bR-9h5xqwurUfPsOR9V-L_Q1chytIEQZTyhUBsJpxRHI_dD_t8J9AxcIxlXWlMpgje3do1Gal4oHpMH7STqryE-UfKIC0jDd5MBEWMg3LpdOPvkvZewiyJkBpM-46B7rh84pm8lmdcl79KEmmED4aFwu2Ql8hJRhvcxsn4u8dO1Z4p16H2cgeiSV5jox6d10szOcF-YTRob_rVIH56z-PQZqBnlBx8uY3RMxsAqWF-59XBVDayYhJ69B6Edzer04VweRXQbxrrn0cznlFtU9jU66zt44kLbo7zwDFxwjiR8W_sm1o0TUz9joTxRJuzt8HFf2RSUyuBUDI0ltsT5jrjK1nh75_mlfKt3F9lL8Jo8HVlpEcYXOBvksRPdyRADtID-bpZRuy2uIXL6KJzdRPicrL4G3lBWpsurZN4_dDI196g1pYjzeZCy82iYrG33cUmSS-uVOZCn1Z2A0GhQDOwWoEWkj0EZHNuvRyEk3DNuftAA14SociqMVBBC1C2kyoulvTgstTqR9CNDZcwgfZjl6-4_xEBCsOOVs1jM_-Oco4Gcv8YXW1mjXHeq8laWJcsak4yhmuFUoqSwZyCz-PFqqwcd6-85gZQn9WJMYkiYrvswXcyl7pNzvtT19ZJjPdnyC2Mbr2HzRfTAC4gT_ScmjlnZqj_FfT962g4fCGYfnsTdurwwGk27UpPrHlBdgnxBEto5alng6PuAWfjdfdkfMdfunX0_P_Cl5akwD8Pbgkr_NSSXxY_c9zwdrhZOX2uDsLQbFHSicJNAqJz1OL8KSlyeSYiXonVJdAOzg0X8986k9OpFRJpzqrPKJ2taZcp_N3pP2KBuUAh_9sDiuT3aQVINuexcSux5tMY7Nu1vKtzwevCQAYQZPn0ktJjOcQZLmNZm5OhuQy2TDU. Acesso em: 15 nov. 2024.</p>
</div>
<div data-bbox=)