http://doi.org/10.23925/2179-3565.2025v16i4p258-269

RISUS - Journal on Innovation and Sustainability
volume 16, número 4 - 2025
ISSN: 2179-3565
Editor Científico: Arnoldo José de Hoyos Guevara
Editor Assistente: Vitória Catarina Dib
Avaliação: Melhores práticas editoriais da ANPAD

LEVIATÃ OF THE DIGITAL ERA
CONFLICT BETWEEN PRIVACY AND FUNDAMENTAL RIGHTS

Leviatã da era digital: conflito entre privacidade e direitos fundamentais

Marcelo Augusto Vieira Graglia, Celeida Maria Celentano Laporta
Pontifícia Universidade Católica de São Paulo
Email: marcelograglia@yahoo.com.br, advogada@celeidalaporta.adv.br

ABSTRACT

This article aims to determine the effectiveness of society in a digital era taking into consideration the conflict between privacy rights and fundamental rights concerning information access. In view of the interdisciplinarity, a brief history is presented regarding the privacy right, and Technology, making it clear the characteristics, institutes and the impacts of interactive virtual society. The right of personality is a fundamental right, individual right and right of freedom, as such we report a brief history of the right to privacy and thoughts on the right to protection of privacy as opposed to the right to free access to information, with a society that uses In expressive numbers the way of the information, in other words, the Internet supported by its border tentacles that access everything and everything controls. Therefore, analysis of the current Internet governance scenario, regarding the development of rules, principles and procedures common to Governments, the private sector and civil society in relation to the use and evolution of the Information Society.
Keywords: Privacy rights, Interactive digital society, Privacy invasion, Governance

SUBMETIDO EM: 12/12/2025
ACEITO EM: 20/12/2025
PUBLICADO EM: 30/12/2025

RISUS - Journal on Innovation and Sustainability
volume 16, número 4 - 2025
ISSN: 2179-3565
Editor Científico: Arnoldo José de Hoyos Guevara
Editor Assistente: Vitória Catarina Dib
Avaliação: Melhores práticas editoriais da ANPAD

LEVIATÃ DA ERA DIGITAL
CONFLITO ENTRE PRIVACIDADE E DIREITOS FUNDAMENTAIS

Leviatã of the digital era: conflict between privacy and fundamental rights

Marcelo Augusto Vieira Graglia, Celeida Maria Celentano Laporta
Pontifícia Universidade Católica de São Paulo
Email: marcelograglia@yahoo.com.br, advogada@celeidalaporta.adv.br

RESUMO

Este artigo tem como objetivo determinar a eficácia da sociedade em uma era digital, levando em consideração o conflito entre direitos de privacidade e direitos fundamentais relacionados ao acesso à informação. Diante da interdisciplinaridade, é apresentada uma breve história sobre o direito à privacidade e a Tecnologia, deixando claro as características, institutos e impactos da sociedade virtual interativa. O direito de personalidade é um direito fundamental, direito individual e direito à liberdade; como tal, relatamos uma breve história do direito à privacidade e reflexões sobre o direito à proteção da privacidade em oposição ao direito ao acesso livre à informação, com uma sociedade que utiliza em números expressivos o modo da informação, em outras palavras, a Internet sustentada por seus tentáculos de fronteira que acessam tudo e tudo controla. Portanto, uma análise do cenário atual de governança da Internet, considerando o desenvolvimento de regras, princípios e procedimentos comuns aos governos, ao setor privado e à sociedade civil em relação ao uso e evolução da Sociedade da Informação.
Palavras-chave: Direitos à privacidade, Sociedade digital interativa, Invasão de privacidade Governança

INTRODUCTION

This article aims to analyze the aspect of information control and management, as well as the invasion of privacy that this digitized universe causes in the lives of technology users. Information belongs to everyone or to each individual, since information and data are sometimes centralized, sometimes distributed, not always in a rational or legal way.

The world has witnessed a formidable technological revolution in recent decades; the spread of information technology has produced profound social, economic, political, and cultural transformations, both nationally and internationally (Lazzareschi; Graglia, 2023). The labor market is being increasingly transformed by digital technologies, generating new challenges and social, ethical, and economic impacts (Graglia, 2018). Computer tools have penetrated and generated changes in society and consequently in the rules and laws that govern it, moving between two sciences: Technology and Law.

Thomas Hobbes (1999), in the 18th century, created the concept of Leviathan, the biblical monster that, in a metaphorical view, represented the State, protector and holder of a social contract that established peace, with its tentacles controlling and guaranteeing the rights and duties of individuals, after all, the world needed to evolve and society needed order to track this evolution where men would renounce war against other men. And as the world evolved, in parallel, a new Leviathan was incorporated: the Leviathan of the digital age, automated and controlling the channels of information, data, images and audio.

Digital Law emerges with paradigms such as the right to information, the right to privacy of citizens and companies, respect for the privacy of third parties and the fundamental rights of each individual. In the digital age, a protection of rights emerges where information is distributed indiscriminately; Internet, social networks, databases, tracking, digital signature, culminating in the convergence of public and private information. The biggest challenge lies between the speed of innovation and the inertia of the law in legislating on social networks, telecommunications, e-commerce, and access to distributed databases.

With regard to privacy, the following topics were analyzed from a legal perspective: history of the right to privacy, characteristics of the right to personality, and protection of speech, image, and intimacy. Furthermore, an attempt was made to draw a line of convergence to analyze and write about privacy in the digital age in light of questions and research on: limits of the fundamental right to freedom and the right to privacy, social networks, e-commerce, email, and crimes against privacy on the internet.

Finally, given the deductive methodology, this brief article focused its research on observing concepts and questions in order to define the collision between the right to privacy and fundamental rights in the digital age.

1 INTERACTIVE DIGITAL SOCIETY

In Digital Law, information is its raw material, belonging to the category of intangible assets, information that can be traded, archived, manipulated, valued, and illicitly obtained. Along these lines, the Law has evolved, encompassing institutions, fundamental principles, and legislation as a framework to support the interactive digital society. Digital interactivity is a kind of intersocial relationship, that is, a dialogue between man and machine, which enables interaction with the tool and with the information. As for legal professionals, even though many are hesitant about technology, it is no longer possible to avoid the technological advent and its impacts on their profession and their clients. It is necessary to provide legal services in the areas of contract drafting and litigation regarding copyright, intellectual property, image rights, information security, social network intrusion, royalties, and e-commerce.

Paesani (2003) teaches that information technology and its tools penetrate society in such a way that they have modified interindividual relations, so that information has become a new legal asset of modern man, which hovers between a lack of technological knowledge on the part of jurists and a lack of legal knowledge on the part of information technology professionals. In view of this, Digital Law must be understood and studied in a way that it can innovate and develop the institutes, laws and procedures necessary to meet the needs of this dichotomy of cultural knowledge.

The advent of the globalization of the economy and society corollarily imposes the globalization of legal thought, in order to find mechanisms for applying norms that can go beyond the principles of territoriality. In the

globalized world, everyone is connected in a single village, technology has overcome the barriers of distance and territoriality. This trend of globalization can be observed through International Conventions and Treaties, which establish criteria and standards for legal analysis in the face of border barriers. The information that travels through a complex network of protocols promotes an interactive digital society, and the speed of technological advances is proportional to the speed of information transmission. Thus, as Casimiro (2000) argues, this interactivity requires that virtual companies be prepared to serve consumers and users anytime, anywhere. Furthermore, as stated in the scientific work of Laporta (2011):

> "For companies to have an open channel of communication with the digital world, much more is required than just selecting the target audience or other management concerns, but rather the creation of a legal framework that reflects the cultural diversity of virtual consumers and the respective guarantees of this legal relationship.All this technological-social movement brings some consequences that must be resolved, such as maintaining the right to privacy and guaranteeing the right to information, emphasizing that Brazil is a signatory to international treaties and conventions, such as the Universal Declaration of Human Rights."

In the face of an interactive digital society, one of the great challenges of Digital Law is to be prepared for the unknown, with the capacity to interpret, understand, and adapt to the reality and customs of a globalized and interconnected society in the face of the respective impacts on specific cases, which are caused in legal relationships that must be regulated by valid and effective norms in virtual matters.

1.1 Legal institutions and their terminology

In the construction of an interactive digital society, every hypertext-multimedia protocol relationship, whether resulting from human actions or machines, implies rights, duties, obligations, and responsibilities. The construction of legal institutions is essential for building a shield for businesses against the risks that technological treatment entails in these relationships.

Similarly, for Paesani (2003), Law is responsible for balancing the behavior-power relationship, which can only be achieved through the proper interpretation of social reality, creating norms that guarantee the security of expectations through their effectiveness and acceptability, that understand and incorporate change through a flexible structure that can sustain it over time. And he adds:

"The relationship between law and computers is profoundly different from the relationship between law and any other machine on the market. Digital law is interdisciplinary, as it simultaneously affects numerous fields of law."

This transformation leads us to Digital Law, which advances every day, encompassing all the fundamental principles and institutions that are in force and, moreover, creating new ones. Because it is an interdisciplinary field, Digital Law is established in various areas of law, be it Civil Law, Copyright Law, Commercial Law, Tax Law, Labor Law, Criminal Law, and, as a consequence, introduces new institutions and elements to legal thought. Virtual companies, providers, copyright, email, information security, trademarks and domains, digital signatures and digital certificates, among the legal institutions that are formed within digital law, it is worth highlighting, as Blum (2001) teaches about electronic commerce:

“There is a long way to go. With the global growth of the Internet and computer-based business, doubts and problems regarding the commercial application of this new technology are also growing. One of the great questions in human history has always been the search for certainty regarding the authenticity of documents and even people. If this was already the case with papers and people within our reach and sight, what can be said now that our business partners are only names on a computer screen?”.

Furthermore, according to data released by the Brazilian Institute of Geography and Statistics (IBGE), the number of internet users and the growth of e-commerce in Brazil are significant. According to the PNAD TIC survey, in 2021 Brazil had 155.7 million internet users, present in 90% of Brazilian households. In approximately 99.5% of these households, internet access was via mobile phones, in 44.4% via TV, and in 42.4% via computer (Nery; Britto, 2021). According to the Webshoppers survey, 47th Edition, conducted by Nielsen NIQ Ebit (2023), e-commerce in Brazil generated R$ 199.1 billion in 2020 and R$ 258.5 billion in 2021, indicating a growth of 29.8%. In 2022, the amount transacted grew slightly more, reaching R$ 262.7 billion.

Observing this scenario reveals a common thread for a society of online users who are accustomed to accessing online platforms and mobile applications. These users inevitably make their personal information available and access much more. These are just some of the situations that are already being legally observed, among others: cybercrimes, e-learning, interactive TV, online advertising, virtual auctions, virtual finance, all with legal implications for both the right to information and the right to privacy. Numerous concepts and terminologies are used for such an impetuous field, which accompanies the Law in the evolution of technology: Information Society Law, Electronic Law, Computer Law, Internet Law, Cyber Law and Digital Law. Based on the understanding of CASIMIRO (2000):

"The globally used term is Information Society, that is, a society where information is considered a primary and indispensable strategic resource for its own development; a society that prioritizes the rapid and effective transmission of information."

The terminology used by doctrinators varies; however, the overarching concept prevails: they should represent a society where information is listed as one of its greatest legal assets, an indispensable element for the development of a society where priority is given to the timeliness, speed, and effectiveness of access to and transmission of information, which is in continuous development.

2 FUNDAMENTAL RIGHTS TO PRIVACY

Law has the function of protecting the interests and legal assets of society so that it may live, coexist and survive in harmony, and its objective is to regulate the interaction of people with other people in the world, according to the terminologies of justice, personality and humanity.

Brunello Stancioli (2003), from the Federal University of Minas Gerais (UFMG), teaches in his article published on the internet the origin of the concept of person:

"It is correct to say that the terms concerning *personality* were already circulating among the Romans and the Greeks. According to Boethius, *persona* – along with its Greek equivalent *prosopon (Prosvpon)* – designated the mask used in the theater. Through this mask sounded louder, the actor's voice. In another sense, this mask (*persona*) always evoked the role played by the actor. It was the person, the figure represented, the character or even the personality:

The name of persona, in fact [...] comes from those who represented, in comedies and tragedies, the figures who offered the pertinent interest. In fact, *persona* comes from *personando* [*personare*: *per* – much, with strength, and *sonare* – to sound]. It will be clearly seen that this word comes from *sonus* [sound]. It is certain, for this reason, that the sound then produced is necessarily stronger, as a result of the concavity itself [of the mask].

Thomas Aquinas, referring to Boethius, uses the same metaphor as the etymology of person, when he states that "the term *persona seems to* derive from the masks that represented human characters in tragedies". The notion of "mask" and "paper" is, even today, pertinent in this sense of:

To represent the conception we have formed of ourselves – the role we have striven to play – this mask is our truest self, the self we would like to be [...]. We come into the world as individuals, we gain character, and we become people."

Based on Laporta's research (2011), the right to personality is related to the position of human beings in Law, with the requirement of their dignity. The subjective right to personality has a unity, which stems from the unity of the person and their dignity. The holder of the right is one, and their dignity is also one, that is, highly personal. The right to personality is a fundamental right, an individual right, and a right to freedom, and these expressions are synonymous and complementary. In short, what really matters is the common core that everyone protects: the person.

Alexandre de Moraes (1998) describes that the Law of the Twelve Tables can be considered the origin of written texts enshrining freedom, property, and the protection of citizens' rights, and teaches that Roman Law established a complex mechanism to protect individual rights. In the same vein, it is appropriate to cite Bruno Stanciolli's article (2003) on the creation of the right to personality, which was created by the Federal Supreme Court of Germany in the 20th century. Personality rights are absolute, essential, inalienable, and non-transferable. They are acquired at birth and generally end with death. These include the rights to one's own life, image, freedom of expression, protection of one's name, and the inviolability of private life.

2.1 History right to privacy

Legal norms represent, throughout history, the evolution of society and its needs. These norms were born over time with the following legislations: Code of Hammurabi, Mosaic Legislation, Code of Manu, Law of the XII

Tables, The Koran, The Magna Carta, On Crimes and Punishments, Declaration of the Rights of Man and of the Citizen and Universal Declaration of Human Rights. Although these codes regulated with much punishment, they always preserved honor, name and word. As an example, in the case of crimes of injury or insult, the tongue was cut with a red-hot iron stiletto and boiling oil through the mouth as payment of a fine. Through a path of mistakes and successes, wars and revolutions, humanity, on December 10, 1948, in Paris, consolidated, in theory, the most advanced legal thought of humanity, that is, the Declaration of Universal Rights. Nevertheless, the right to intimacy or privacy of the person, which disposes of private life, image, intimacy and secrecy, are correlated to the cultural, social and territorial context in which each person is inserted.

In summary, for Laporta (2011), the Right to privacy is related to all events, facts or situations that the person does not wish to share or make public. It is what most characterizes the individual within his uniqueness and his unique and personal identity, that is, his private life.

2.2 Protection of image, name and intimacy

The right to privacy is delimited by a non-tangible space, which makes up the principles and values of each person's private life. There are no boundaries between physical and/or psychic threats and, as indivisible and inalienable legal assets, the image, name and intimacy of the person must be protected.

The invasion of privacy is an old thing, according to Blum (2001):

"The invasion of privacy is an old thing, it comes from time immemorial, it is correlated with the search for information. In the Renaissance, the Florentine Machiavelli, a cynic, in the philosophical sense of the word, coined a phrase that became famous, precisely because it synthesizes the reason for this search: whoever has the information, has the power. If before the information was disconnected from each other, now, the intersection is total, at a speed in the rhythm of bytes, in the already outdated concept of the global village advocated by Herbert Mcluhan."

Furthermore, it is incumbent upon the Brazilian Magna Carta, under the terms of its article 5, to ensure, preserve and protect these rights that are inviolable to intimacy, private life, honor and image. The concepts of intimacy and private life are tenuously interconnected and, for Alexandre de Moraes (2008), intimacy and private life are differentiated between subjective and objective relations. In an analysis of the distance between intimacy and private life, Mendes (1999) clarifies Hubmann's (1953) German theory of spheres, in his famous work *Das Personlichkeitsrecht,* which classified the general right of personality into three circles or concentric spheres:

"In the larger sphere, the private sphere, events that the individual does not want to become public take place. Outside this sphere are the occurrences and conducts of a public nature, within the reach of the community in general, and crimes of indiscretion do not apply.

The sphere of intimacy, or confidential sphere, is contained in the private sphere; it is a closed circle in which only very close people participate.

Finally, more in the center, is the sphere of secrecy, which must be protected from every form of indiscretion. Not even the people of the subject's intimacy participate in this sphere; the need for protection against indiscretion is more intense."

The right to privacy, both in its larger sphere, which contains the public facts of the citizen's life, and in the smallest, which is the sphere of intimacy with people's most intimate information or even in its center, where the sphere of secrets is housed, even if protected by the legal system, are rights that are notoriously threatened in the face of the invasion of privacy in the digital age, A cyberspace where everything is known, everything is seen and everything is controlled.

3 IMPACTS OF ACCESS TO DIGITAL INFORMATION

On the other hand, access to information is also a fundamental right, provided for in the Brazilian legal system in article 5, item XXXIII, as well as in item II of paragraph 3 of article 37 and paragraph 2 of article 216 of the Federal Constitution of 1988. Faced with the desire for information at any time, in a cyberspace where technology is transformed every second, it is necessary to consider the generations that are born in this environment, currently the "Generation Z" or also called the "post-millennial" generation or even "descendants of digital natives", generations that decide, consume, disseminate and live under the aegis of digital information, especially with their smartphones. According to a survey by Exame Magazine (Caleiro, 2015), "generation Z" in the United States makes up an army of 70 million people, that is, about 22% of the population. With the popularization of smartphones, in the short term, practically everything will be done in the virtual world. However, consumers will be increasingly

concerned about their privacy, whether in payments, transactions or searches for products and services. It is well known that users do not want companies to have all their information after purchasing or accessing some survey. Given this, there will be a growing search for websites, apps, and tools that allow users to make user information more discreet and confidential.

Access to information crosses the boundaries of intimacy and often devastates people's private lives, to the extent that almost everything is just a "click", a "like" or an "enter" away. For Peck (2011), the limit between access to information and the right to privacy has to be equated, weighing the commercial interests, privacy, responsibility and anonymity generated by the new technological vehicles. And he also teaches:

> "There is no legal gap regarding the solution of privacy on the Internet. There is, however, a lack of understanding as to the explanation of laws in force for relatively new issues, which require interpretation of the rule and its adequacy to the specific case. This is a fundamental principle for the application of the Law, and, consequently, it must also be adopted in Digital Law."

Along the same lines, Casimiro (2000) teaches that the need for rapid access to information, as well as the use of this information, has led to the conclusion that the internet corresponds to the *information highway*, which makes it possible to find the appropriate information for each need. The internet in the US has been dubbed the "*information superhighway*" and questions whether the current legal order is prepared to solve the difficulties arising from these virtual information highways.

And, through these roads, different paths and tools are chosen to access information and communicate, whether through e-mails, e-commerce, Facebook, spyware, Instagram, LinkedIn, WhatsApp, Skype, Google Hangouts, programs to access government systems, banking information, among many others and, with them, the impacts: spyware, spam, cookies, worms and hackers, who invade and kidnap information, they disrupt people's privacy, whether within the private, public, or secret sphere.

For Crespo (2011), *spyware* is a simple way to obtain information; they are spy files that track user information contained in their computer. Cookies are also found, which are nothing more than a file that stores information exchanged between browser and server, in order to provide speed to computer access, which is due to the lack of need to enter some data when there is access to a certain page again.

Worms are viruses that are smarter than the others, which contaminate as many computers as possible, identifying the flaws of the applications installed on the user's machine; Hijackers, on the other hand, are viruses that hijack internet browsers and change the user's browser. With these tools, for example, private materials or facts are captured without the victim's consent (Pfizer, 2016).

Regarding social relationship networks, Basso (2008) explains that their impacts and their stabilization in the virtual space are defined as structures constituted between individuals and groups or organizations in a given space, connected from personal bonds (family, emotional, professional or ideological, for example), varying between formality and causality, in a random or orderly way. And he adds that:

"**Internet social relationship networks** , due to the reach of their structures and high degree of inclusion of users (measured by criteria of association or adhesion), also **end up giving rise to the erosion of privacy within and from the Internet**. Individuals in an affinity group are encouraged to observe and monitor the behavior of other members in their social life activities. **"(Emphasis added**).

Social networks create autonomous rules, enable and make available content and personal information, such as names, photos, addresses, texts, as a rule, without any consistency or protection. In this line, it is worth highlighting the book "Faceboom" by Juan Faerman (2011), when he explains that the information contained in social networks is raw material par excellence for neighborhood gossip in the twenty-first century, and contextualizes what social networks are for: **"Tell me all the information about you and I will tell you who you are" (emphasis added)**

3.1 Internet governance landscape

The issue of the right to privacy and access to information, in the face of this gigantic network of networks that we call the internet, is extensive and controversial. These are rights to be protected for both individuals and

legal entities, involving a web of knowledge and complex theories in the face of the interdisciplinarity of the subject. In this way, internet governance is as eminent for companies, governments, non-governmental institutions as it is for any connected citizen, considering that, in an interactive digital society, resources are indispensable for their corporate or personal development in the world market. Controversies have already begun regarding the definition of the topic of internet governance, according to the CGI – Internet Steering Committee in Brazil (2018). In the publication of the booklet "An Introduction to Internet Governance", Kurbalija (2016) describes:
"The controversy surrounding Internet governance begins with its definition. It is not just about linguistic pedantry. The way the Internet is defined reflects different perspectives, approaches, and policy interests. Traditionally, telecommunications specialists have viewed Internet governance from the perspective of developing a particular technical infrastructure. Computer specialists focus on the development of different standards and applications, such as XML (eXtensible Markup Language) or Java. Communication experts emphasize ease of communication. Human rights activists view Internet governance from the standpoint of freedom of expression, privacy, and other basic human rights. Lawyers focus on jurisdiction and dispute resolution. Politicians around the world often prioritize issues that resonate with their electorate, such as techno-optimism (more computers = more education) and threats (Internet safety, child protection). Diplomats are primarily concerned with the development of national interests and their protection."

After overcoming the initial barriers, the WSIS[1] – World Summit on the Information Society presented the following definition of Internet governance, by Kurbalija (2016) as: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of principles, norms, rules, decision-making procedures and common programs that define the evolution and use of the Internet." The main points addressed in the WSIS are about technical coherence and normative aspects, considering actors from the business sector and governments, with different political and economic interests, an issue that still remains open, being relevant to the next topics of the debate on the future of internet governance. Another point highlights the discussion about the decentralized structure versus the centralized structure of internet governance. This item is complex, although supported by the technical community of the Internet and by developed countries, as the Internet cannot be placed under a single governance. As a central item, it deals with the protection of public interests on the internet, the way in which the public nature of the internet prevails over the others, and this issue is open, strengthening net neutrality. As for other premises, such as Geography and the Internet, the WSIS understands that the more the Internet is based on geography, the less unique its governance is achieved, which causes another controversial point: jurisdiction on the Internet. Furthermore, regarding issues that concern freedom of expression versus protection of public order – the well-known debate between article 19 (freedom of expression) and article 27 (protection of public order) of the Universal Declaration of Human Rights – it is clear that the discussion is frequent in the context of content control and censorship on the internet. The themes and paradigms still have many open questions, especially cybersecurity and human rights, as stated in the booklet "An Introduction to Internet Governance", by Kurbalija (2016), where he states that more security implies less human rights and opposite.

At the same time, the CGI.BR, the Internet Steering Committee in Brazil, promotes studies and recommends procedures for Internet security, having defined that the principles for the governance and use of the Internet are: Freedom, privacy and human rights; Democratic and Collaborative Governance; Universality; Diversity; Innovation; Net neutrality; Non-imputability of the network; Functionality, security and stability; Standardization and interoperability and legal and regulatory environment. In summary, the violation of the protection of intimacy and the right to free access to information face constant technological, political, cultural and territorial difficulties. However, it is necessary to seek the convergence of interests, the preservation of human rights and international cooperation on the criteria and the standardization of legislation and governance on the Internet.

[1] UN General Assembly Resolution 56/183 (December 21, 2001) approved the holding of the World Summit on the Information Society (WSIS) in two phases. The first phase took place in Geneva from 10 to 12 December 2003 and the second phase took place in Tunis from 16 to 18 November 2005. The aim of the first phase was to develop and foster a clear declaration of political will and to take concrete steps to lay the foundations for an information society for all, reflecting all the different interests at stake. More than 19,000 participants from 174 countries attended the meeting and related events. Source: http://www.itu.int/wsis/basic/about.html [accessed January 21, 2024].

3.2 Artificial intelligence, IoT, and increased complexity

The creation of the internet can be seen as a great innovation, which had not only a substitute effect, but a revolutionary one. The effects of the creation of the internet still reverberate in today's society, modifying the economy, culture, productive arrangements, educational systems, and forms of organization of society. But the internet is not an isolated innovation. New technologies with similar potential have been emerging and evolving, especially the so-called digital technologies. In the early decades of the twenty-first century, innovations such as artificial intelligence, blockchain, virtual and augmented reality have spread intensely and rapidly, challenging social structures, institutions, organizations, and individuals (Graglia; Figueiredo, 2021). It seems that there is a temporal convergence, as they are reaching a certain degree of maturity relatively simultaneously. Some derive from the internet itself, or at least are made possible from it, while others do not keep this relationship.

This convergence accentuates the possibility of major impacts. At the same time, it makes it difficult to build future scenarios, due to a more complex composition of interaction, applications and effects. This phenomenon is accelerated by a real race of organizations and companies that seek to undertake innovation and digital transformation processes in search of greater competitiveness (Graglia; Huelsen, 2023).

IoT – Internet of Things

The term "Internet of Things" (IoT) was coined by British expert Kevin Ashton (2009) in a presentation to Procter & Gamble executives in 1999, when he talked about the idea of electronically tagging the company's products through radio frequency identifiers (RFID) to facilitate production chain logistics (FINEP, 2015). With RFID tags, it is possible to electronically track products and vehicles, obtaining information about their geolocation. IoT is beginning to be made possible at scale with IPv6 (version 6 of the internet protocol), which allows the almost unlimited combination of codes (or protocols) enabling the identification of a massive amount of objects, equipment, machines and other devices. Thus, technically it is possible to identify and track every appliance, automobile, computer, telephone and other existing product. In addition to identification and tracking functions, these *chips* associated with computing systems make it possible to connect devices that are not yet intelligent with other devices and systems, so that they can interact autonomously with each other. Automobiles, houses, offices, buildings, and traffic lights can be connected, which generates countless possibilities for services, benefits, and information. Data generation is a critical aspect of the internet of things. Gigantic volumes of data are available, which allows the analysis of behaviors, frequencies, volumes, routes, consumption preferences, energy expenses, among many other possibilities, in the most different fields of application: social, scientific, military, commercial, etc. Associated with sensors, they allow the remote control of devices and their effective performance in the physical world (Graglia, 2018). One of the business models structured from the internet of things and in a significant process of expansion is the so-called Industry 4.0, a model that modifies the logic of industrial production based on the intense use of digital technologies, sensors and robotics in an integrated arrangement with the management systems of the factories, the so-called vertical integration, and also from the integration between companies in the same supply chain. This model has great potential to impact the productivity levels of the countries that best implement it (Graglia; Figueiredo, 2021).

Artificial intelligence

The term Artificial Intelligence, as we know it today, was coined by Professor John McCarthy, from Stanford University, during the conference he organized at Dartmouth College, in New Hampshire, USA, in 1956. Other scientists also participated, such as Nathaniel Rochester from IBM, Claude Shannon from Bell Laboratories and Marvin Minsky from Harvard University, who contributed to Artificial Intelligence becoming a field of study. However, the development and expansion of the application of this technology proceeded more slowly than expected due to existing technological constraints, such as limited computing power, low data availability, and the level of development of machine learning algorithms. The early 2000s, on the contrary, marked the acceleration of the development of artificial intelligence and the emergence of numerous applications, such as the application of artificial intelligence in robots, such as the cleaning robots produced by the company iRobot and the robots of the company Boston Dynamics, capable of walking on different types of rough terrain (with snow or stones, for example) and perform various tasks. From 2008, natural language processing (NLP) advances and one of the commercial applications is voice recognition for searches, launched by Google to operate on Apple's iPhone. In

2011, the first virtual assistant system is launched on the market: Apple's Siri, capable of answering questions, doing searches, etc. Then Amazon launches Alexa and others follow. Another emblematic event that occurred in 2011 was the victory of IBM's Watson supercomputer over two of the greatest champions of a famous quiz show in the United States, Jeopardy. In recent years, one of the main evolutions has taken place in the field of so-called generative artificial intelligence, a type of AI capable of generating texts, sounds, images, and other media. Generative models learn the patterns and structure of the input data and generate new content, in a kind of creative work. Generative AIs are based on algorithms called LLMs, or large language models, which consist of neural networks with many billions of parameters, which are trained on huge amounts of data, usually through unsupervised or semi-supervised learning processes. They are general-purpose models and serve a wide range of tasks, from sentiment analysis, pattern recognition, and mathematical reasoning. Among the main generative AI systems today, we can mention ChatGPT developed by OpenAI, Bard developed by Google, Midjourney and DALL-E. The expansion of the use of predictive artificial intelligence systems and the emergence of generative artificial intelligence systems have produced significant transformation in several fields of human society (Graglia et al., 2024). The concrete possibility of expanding connectivity and increasing the generation, use and transaction of data by arrangements such as the Internet of Things and artificial intelligence, indicate a clear trend towards an increase in the complexity of the issue and the urgency of applying ethical principles and specific regulation, to avoid the escalation of occurrences of violation of privacy and fundamental rights (Graglia; Huelsen; Lazzareschi, 2021).

CONCLUSION

Information, since the dawn of humanity, has always been a precious legal asset, a heritage that represents and includes the power and control of information knowledge. Throughout history, it is noticeable that societies have always been risky and, with the Information Revolution from the twentieth century, it would be no different. Great evolutions have emerged as a result of this technological advance, both in the social and scientific areas. However, major problems have also arisen for this new interactive digital society. In the face of evolution, the world has coexisted with a revolution of globalization and technology at a level of interactivity never seen before, with information having migrated from handwritten to digitized form. Information and knowledge were available at a click. This process implied a significant change in the behavior of individuals, government agencies and national and international companies, to the extent that this new world scenario presented a compendium of complexities, especially the collision of interests and principles, on the one hand the right of access to freedom of digitized information and, on the other, the right to privacy.

Nevertheless, the core of the matter focuses on how Law will regulate the digital society, in the face of conflicts of a new society, in which human relations are in constant transition and become increasingly interactive. Millions of people, considering the speed and interconnectivity of globalized information on the internet, yearn for the right to information and the right to be informed, as long as freedom of expression, protection of name, word, image, in short, the inviolability of private life are guaranteed. And then a biblical figure emerges to metaphorically represent this scenario of cyberspace: the Leviathan monster that, with its tentacles, controls all information, whatever it is, wherever it is, and also brings to light the legal insecurity with the main threatened good, that is, the privacy of the user of the digital society. In fact, the guarantee of human rights must be a priority before all nations, and the right to privacy is fundamental to preserve the expression of thought and for the survival of democracy, whether in the virtual world or not. At the same time, the responsibility lies with all individuals, whose primary mission is to practice and defend the principles of human dignity.

REFERENCES

Ashton, K. That "Internet of Things". [S.I.]: *RFID Journal*, 2009. Available at: http://www.rfidjournal.com/articles/view?4986. Accessed on: 20 jul. 2025.

Basso, Maristela. In: Lucca, N., Simão Filho, A. *Law & Internet. Relevant Legal Aspects Vol. II.* São Paulo: Editora Quartier Latin, 2008.

Blum. R. O. *Electronic Law.* São Paulo: Edipro, 2001.

Caleiro, J. P. *Forget millennials: Generation Z is coming*. Available at: https://exame.abril.com.br/economia/esqueca-os-millenials-a-geracao-z-vem-ai/, Accessed on 10 jul. 2025.
Casimiro, S. de V. *Civil Liability for the content of Information Transmitted over the Internet.* Coimbra: Almedina, 2000.
CGI.BR. *Principles for Internet governance and use.* Available at https://www.cgi.br/principios/. Accessed on 20 May. 2025.
Crespo, M. X. de F. *Digital Crimes*. São Paulo: Editora Saraiva, 2011. Graglia, M. A. V., Huelsen, P. *Innovation and Competitiveness*. São Paulo: Editora Senac São Paulo, 2023.
FINEP. *Kevin Ashton – interview with the creator of the term "Internet of Things".* Rio de Janeiro: Finep, 2015. Available at: http://finep.gov.br/noticias/todas-noticias/4446-kevin-ashton-entrevista-exclusiva-com-o-criador-do-termo-internet-das-coisas. Accessed on: 12 jul. 2025.
Graglia, M. A. V. *New technologies and mechanisms of impact at work*. 2018. 330 f. Thesis (Doctorate in Intelligence Technologies and Digital Design) - Graduate Studies Program in Intelligence Technologies and Digital Design, Pontifical Catholic University of São Paulo, São Paulo, 2018. Available at: https://repositorio.pucsp.br/jspui/handle/handle/21157. Accessed on: 2 Dec. 2025
Graglia, M. A. V., Huelsen, P., Lazzareschi, N. The growing moral challenge in the face of technologies: internet, social networks, IoT, blockchain and artificial intelligence. *In: RISUS – Journal on Innovation and Sustainability*, São Paulo, v. 12, n.2, p. 17-29, abr./ mai. 2021. Disponível em: https://doi.org/10.23925/2179-3565.2021v12i2p17-29. Acesso em: 2 jul. 2025.
Graglia, M. A. V.; FIGUEIREDO, A. R. Industry 4.0 in Brazil and the challenges of the productivity of the economy. *RISUS – Journal on Innovation and Sustainability*, São Paulo, v. 12, n.4, p. 13-28, out. / nov. 2021. Disponível em: https://doi.org/10.23925/2179-3565.2021v12i4p13-28. Acesso em: 4 dez. 2025
Graglia, M. A. V.; Huelsen, P.; Muniz, A.; Valente, C. (ed.). *Artificial Intelligence: understand how AI can impact the job market and society*. Rio de Janeiro: Brasport, 2024.
Hobbes, T.. *Leviathan or matter, form and power of an ecclesiastical and civil state*. São Paulo: Nova Cultural, 1999.
Kurbalija, J. *An introduction to Internet Governance.* Available at: https://cgi.br/media/docs/publicacoes/1/CadernoCGIbr_Uma_Introducao_a_Governanca_da_Internet.pdf . Accessed on 12 jul. 2025.
Laporta, C. M. C. *The Leviathan of Information: The threat to the right to privacy in the digital age.* Final Paper of Undergraduate Course in Law. - Anhembi Morumbi University. 2011.
Lazzareschi, N., Graglia, M. A. V. (Org.). *Transformations in the world of work: tensions and perspectives*. São Paulo: EDUC, 2023.
Mendes, M. G. de O. M. *Right to Intimacy and Telephone Interceptions.* Belo Horizonte: Livraria e Editora Mandamentos, 1999.
Moraes, A. de. *Constitutional Law*. São Paulo: Saraiva 2008.
Moraes, A. de. *Fundamental Human Rights: comments on articles 1 and 5 of the Constitution of the Federative Republic of Brazil.* São Paulo: Atlas, 1998.
Nery, C., Britto, V. Internet is already accessible in 90.0% of the households in the country in 2021. In: IBGE – Brazilian Institute of Geography and Statistics. IBGE News Agency. Rio de Janeiro, 16 Sept. 2022. Available at: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021. Accessed on: June 4, 2025.
NIELSENIQ EBIT. 47th Ed. Webshoppers. Feb. 2023. NIQ Ebit. Available at: https://nielseniq.com/global/pt/landing-page/ebit/nielseniq-ebit-brasil/webshoppers/. Accessed on June 4, 2025.
Paesani, L. M. *Law and the Internet.* São Paulo: Atlas, 2003.
Peck, P. *New Laws for the Digital Society*. Published in 2011. Available at http://www.parana-online.com.br/canal/direito-e-justica/news/560480/?noticia=NOVAS+LEIS+PARA+A+SOCIEDADE+DIGITAL, Accessed on 05 Dec. 2025.
Peck, P. P. *Digital Law.* São Paulo: Editora Saraiva, 2002.
Pfizer, E. *Studies, legislation and information on Privacy in the digital age*. Available at: https://ergapfizer.jusbrasil.com.br/artigos/404937864/estudos-legislacao-e-informacoes-sobre-a-privacidade-na-era-digital. Accessed 20 jul. 2025.

Stancioli, B. *On the Rights of Personality in the New Brazilian Civil Code.* Published in 2003. Available at: http://www.hottopos.com/videtur27/brunello.htm, Accessed on 24 Jul. 2025.