


THE CONSTRUCTION OF A SUSTAINABLE DIGITAL ENVIRONMENT THROUGH PUBLIC POLICIES TO COMBAT CYBER RISKS AND PROTECT CONSUMERS

 <https://doi.org/10.56238/sevened2024.037-209>

Antônio Carlos Efing¹, Cinthia Obladen de Almendra Freitas² and Willian Ryutaro Kobe³.

ABSTRACT

The digital environment, or cyberspace, is an immaterial dimension that integrates social, economic, and technological aspects, being challenged by the excessive exploitation of data and hyperconnection. These factors generate significant risks for individuals and society, especially with regard to the protection of fundamental rights, such as privacy and security in the digital environment. This study investigates how to address these risks, focusing on the normative articulation between the Consumer Protection Code (CDC), the General Data Protection Law (LGPD) and the National Environmental Policy (PNMA). The proposed hypothesis is that, through this integration, combined with the promotion of cyberdemocracy, it is possible to restructure public policies that protect digital rights and promote the responsibility of the agents that cause harm. The methodology adopted is hypothetical-deductive, based on bibliographic research, with analysis of theoretical concepts about the digital environment, risks and the role of information and communication technologies (ICTs). The research also explores digital democracy as a way to overcome normative fragmentation and broaden public debate on digital environmental issues. The objective is to contribute to the strengthening of cyberspace governance and promote balanced socio-environmental development.

Keywords: Digital environment. Sustainability. Public Policies. Cyber Risks. Consumer Protection.

¹ Dr. and Master from PUC/SP. Full Professor at the Pontifical Catholic University of Paraná - PUC/PR, where he teaches undergraduate, specialization, master's and doctoral degrees. Professor at the School of Magistracy of Paraná - EMAP. President of the Consumer Law Commission of the OAB/PR. Member of the Special Commission on Consumer Law of the Federal Council of the OAB. Coordinator of the research group Consumer Law and Technological Society at PUC/PR and CNPq directory. Lawyer.

E-mail: antonio.efing@pucpr.br

² Dr. in Informatics from PUCPR. Full Professor at the PUCPR Law School and Permanent Professor of the Graduate Program (Master's/Doctorate) in Law (PPGD) at PUCPR. Member of the Data Protection and Digital Law Commission of OSB/PR. Member of the Board of Directors of the National Institute for Data Protection (INPD).

³ Bachelor of Laws from PUCPR. Master's student at the Graduate Program in Law (PPGD) at the Pontifical Catholic University of Paraná (PUCPR).



INTRODUCTION

The digital environment, also described as cyberspace or techno-biosphere, represents an immaterial dimension of the environment that transcends physical borders and integrates social, economic, and technological aspects. In this context, unique challenges arise related to the balance of this digital ecosystem, marked by excessive data exploitation and hyperconnection, which generate significant risks for both individuals and society. The central problem that guides this study is how to face the risks that cause imbalance in the digital environment, which affect individuals simultaneously as consumers, data subjects and holders of diffuse rights related to a balanced environment.

The hypothesis raised is that the dialogue of the sources between the Consumer Protection Code (CDC), the General Data Protection Law (LGPD, Law 13.709/2018) and the National Environmental Policy (PNMA, Law 6.938/1981), combined with the promotion of effective cyberdemocracy, can contribute to the restructuring of public policies aimed at facing these risks. This normative articulation not only enables the accountability of agents that cause damage, but also encourages the creation of concrete solutions that promote the protection of fundamental rights, such as privacy (it should be noted that the concept of privacy in this context transcends the consumerist relationship and encompasses other legal relationships (Misugi et al. 2016, p. 432) and security in cyberspace.

The methodology adopted in this work is of a hypothetical-deductive-deductive order, supported by bibliographic research. Initially, theoretical concepts and legal foundations related to the digital environment, risk theory and the role of information and communication technologies (ICTs) were analyzed. From this theoretical basis, practical and integrated solutions were deduced, focusing on normative articulation and social participation.

The research also seeks to explore the role of digital democracy as an instrument to overcome normative fragmentation and broaden the public debate on digital environmental issues. In this sense, it is discussed how ICTs can promote participatory digital citizenship, essential for the formulation of public policies that balance technological advancement and the protection of rights.

This work intends, therefore, to contribute to the legal and political field by proposing strategies that articulate norms, technologies and citizenship to face the challenges of the digital environment. From this approach, it is expected to foster a critical and purposeful discussion that strengthens the governance of cyberspace and promotes a balanced and sustainable socio-environmental development.



DIGITAL ENVIRONMENT AND RISKS

CONCEPT OF DIGITAL ENVIRONMENT

At the turn of the century, Pierre Lévy (2008, pp. 59-67) already visualized a deep connection between nature and technology, conceiving the "technobiosphere", in which language, as a technique, functions as a catalyst for both cultural and biological evolution, allowing the biosphere to expand into cyberspace, an intangible plane. In this sense, cyberspace is understood as an extension of the environment, here called the digital environment, endowed with legal recognition.

This perspective on the digital environment presents a broad vision, integrating living and non-living elements into ICTs, which amplify their functions and impacts. With the emergence of Digital Law, a legal field dedicated to the intersections between Law and technology, it has become imperative to formulate principles that incorporate values of this microsystem into the legal system, extending to the digital environment the protections granted to the natural environment. In this context, the adoption of the principle of a digitally balanced environment in Digital Law, analogous to the principle of ecological balance in Environmental Law, becomes essential for the analysis of this new phenomenon and its peculiarities.

However, the mere definition of a principle, or simple analogies, is insufficient for an effective understanding of the subject, and it is imperative to incorporate concepts from the classical environment, such as sustainability. Hoffmann-Riem (2021), in this sense, considers Digital Law an autonomous legal branch, highlighting the fundamental role of ICTs in the construction of a new social and legal paradigm. The Internet, as a communicational instrument, affects all spheres of human interaction, from interpersonal relationships to the professional and political spheres (Campos, 2022, p. 257), even transforming the very conception of corporeality, by creating a digital dimension for fundamental rights (Sarlet, 2022, p. 22).

The recognition of fundamental rights in the digital environment, in turn, requires adaptations in Brazilian Law. Thus, Koskenniemi (2022, p. 78) points out that legal fragmentation highlights the need for specialized branches, such as Digital Law, which addresses emerging issues in information technologies and, furthermore, that less exotic compared to other fields, it requires attention, as it deals with social and institutional issues mediated by technology.

In this scenario, Digital Law is consolidated as an autonomous field, focused on emerging technologies and their implications. In this scenario, Coutinho (2014, p. 223) describes the digital environment as a human creation and intangible heritage, symbolized



by the electromagnetic spectrum, whose use should promote sustainable development. Castells (2003, p. 87) reinforces that the Internet, as the main expression of the digital environment, represents a culture that values creative freedom, directed to progress and continuous improvement of this environment, but which are operated by entrepreneurs who often aim only at profit and do not pay attention to the possible consequences of abusive data processing, as follows from the paradigm of surveillance capitalism, addressed by Zuboff as "a logic of single accumulation in which surveillance is a foundational mechanism in the transformation of investment into profit" (2020, p. 69).

Although the environment is indivisible, encompassing all species in a balanced system, its didactic classification facilitates the organization of knowledge and more effective protection in practical situations. Based on this view, the digital environment is an immaterial dimension of the environment, highlighted in this article.

Its intangible and immaterial nature makes it possible for the digital ecosystem to overcome physical barriers, encompassing many individuals who become an integral part of this environment. In this regard, Castells (2003, p. 87) defines Internet culture as a technocratic belief in human progress, materialized by hackers and entrepreneurs who aim to reinvent society and boost the modern economy.

Capra (2006, p. 8), in turn, points out that technological advances have transformed capitalism, attributing a central value to information, which has profoundly altered the digital environment as a space in which this new form of economy manifests itself. However, this integration has also brought negative impacts, such as regional recessions derived from hasty decisions and systemic unpredictability (Capra, 2006, p. 10).

Fluidity, characteristic of digital technologies and commonly observed in this context, is described by Bauman (2001, p. 7) as an intrinsic quality, marked by the ease of adaptation and change. This liquidity translates the digital essence of the Internet, a central element of this study, as the main expression of the digital environment.

The connectivity provided by the Internet has made it ubiquitous in contemporary society. As observed by Cavedon, Ferreira and Freitas (2015, p. 201), "by enabling the storage, transmission and processing of information in digital media, information technology becomes ubiquitous in people's daily lives, bringing together a variety of risks that cannot be easily perceived or identified".

In this way, it is observed that the digital environment is intimately connected to human life in modernity, and, as an ecosystem, it is extremely vulnerable to imbalances resulting from interventions by the agents that operate in it. These induced oscillations can take the form of risks, significantly and negatively affecting cyberspace.



RISK THEORY AND THE DIGITAL ENVIRONMENT

From the advent of computing and the creation of the ARPANET in the 1960s, to the spread of the World Wide Web in the 1990s, the Internet has developed to become a global network that has revolutionized communication, access to information, and interaction between individuals. This advance was driven by technical advances such as digitization and digitalization, as described by Gartner (2024),⁴ in addition to the development of accessible communication protocols and interfaces, which democratized access to information and profoundly transformed contemporary society. However, this expansion has also entailed specific challenges related to hyperconnection, resulting from the ubiquity of the Internet and ICTs.

The specialized literature points out that data are fundamental components of this ecosystem. According to Doneda (2011, p. 94), data are the basis of this immaterial structure, acting as primary elements in the digital environment. In addition, Freitas (2022, p. 238) classifies data and its inherent system as follows: "the term 'data' is so broad that it can even be used conceptually as a policy and social phenomenon, and one can even consider the existence of a data ecosystem", so as to involve "complex organizations of dynamic social relations through which data and information move and transform."

In line with the idea that data is essential for the digital environment, Davenport (1998, p. 19) defines data as "observations about the state of the world", for example: "there are 697 units in the warehouse", so that the "observation of these brute facts, or quantifiable entities, can be done by people or by an appropriate technology". The author adds that "from an information management perspective, it is easy to capture, communicate and store data. Nothing is lost when represented in bits." In its analysis, data can be processed to become information, which, in turn, can be refined and transformed into knowledge, establishing a hierarchy where data is at the base, followed by information and knowledge, until it reaches the level of wisdom, all based on data.

Therefore, data are indispensable elements in the digital environment, providing the basis for the practices carried out in this environment, being constantly collected, stored, and processed, regardless of economic purposes, in a licit or illicit way, constituting a true digital ecosystem. Similar to natural resources, often targets of extractivism, of the physical

⁴ "Digitization" is the process of moving from analog to digital form, also known as digital enablement. In other words, digitization transforms an analog process into a digital form without any change in the type of the process itself. In turn, unlike "digitization", the phenomenon of "digitalization" is the use of digital technologies to change the business model and provide new opportunities for generating revenue and value. It is the process of migrating to a digital business.



environment, data are economically exploited, often excessively, which impacts the balance of the system, as will be addressed in subsequent items.

By analyzing the authors' contributions together, it is evident, therefore, that data are essential components of the digital environment. Based on this information, it is concluded that the digital environment, currently represented by the Internet, has the following characteristics: a) immateriality, as it is configured in a physically intangible space; b) fluidity, since, due to the connection, it allows the rapid traffic of information and is in constant transformation; and c) data as essential components, consisting of the smallest unit of this system, continuously injected in large volume.

Once it is established that the digital environment is a complex and well-structured system, with unique characteristics and properties, it becomes necessary to explore its complexity. Cyberspace is a chaotic system, not in the common sense, but in the scientific context, that is, according to the Science of Chaos. For Gleick (1987, p.16-17), some systems are extremely sensitive to changes in initial conditions, which implies that a small change can cause a significant deviation in the observed results, making prediction practically impossible or leading to unexpected results. Chaos, in this context, does not equate to disorder, but rather the opposite of simplicity. Examples of this include the increase in data traffic by "free" services such as social networks and streaming platforms, which keep users connected for hours, generating widely exploited data for marketing purposes, and resulting in unexpected social phenomena, such as the viralization of content. The relationship between the human mind and the digital environment, social networks and the psychology of memetics demonstrate that even the slightest excitement in the digital environment generates unpredictable and exploitable effects (Capra, 2006, p.26).

This chaotic character is reflected in the oscillations that can be interpreted as risks, originating from human actions, either by the use of technologies created for these purposes, or by decisions made about the treatment of data. Considering that these risks emerge from the intention to exploit data excessively, the applicability of Beck's risk theory, generally applied to the physical environment and global catastrophes, is perceived.

Thus, by recognizing the digital environment as a facet of the broad concept of environment, it becomes evident that it is also subject to risks induced by human action, such as excessive exploitation of data. To correlate digital risks to risk theory, some of Beck's concepts are pertinent. First, the author (2002, p. 78) distinguishes "dangers" from "risks", stating that the former do not result from deliberate choices, while risks are the consequence of decisions for economic and technological purposes that ignore associated threats. Thus, the factors mentioned are not to be confused with natural hazards. In



addition, Beck (2002, p. 84) states that risks are not restricted to time and space, becoming events with a beginning, but without an end. Finally, Beck (2002, p. 86) observes that people do not perceive the risks that surround them, trusting "experts", which, according to the author, generates a feeling of constant uncertainty.

In this way, Beck's conceptions of risk can be applied to the digital environment. Considered a dimension of the environment, the digital environment has its own complex data ecosystem, composed of globally connected devices and subject to human interventions. Beck's theory of risk applies to the digital environment by finding that: a) risks are generated by human actions, often for economic purposes, mainly by companies and even States, as Freitas (2022, p. 228) observes; b) the risks transcend time and space due to the global Internet connection; and c) the risks are almost imperceptible to users, who often have their data collected without knowledge, exposing them to sensory deprivation. Therefore, the characterization of the cyber risks that plague the digital environment is observed.

Considering that the digital environment is subject to risks, it is imperative to adopt measures to mitigate them, especially with regard to the protection of personal data. Freitas (2022, p. 244) states that "the protection of personal data can be an event within the risk analysis [...]". Laws such as the General Data Protection Law (influenced by the European Union's GDPR) seek to provide this protection, but they still have gaps, as will be discussed in subsequent items.

In addition, the imbalance in the digital environment can negatively affect the mental health of users, as demonstrated by the experiment promoted by Facebook (Presse, 2014), in which people were impacted by oscillations in the digital environment. From this interrelationship between technology, mental health, and increased risks, it is understood that the protection of the digital environment is relevant to people's quality of life.

SYMBOLISM OF LAW IN THE FACE OF IMBALANCE IN CYBERSPACE

The analysis of symbolism in Law and Politics is essential to understand how these spheres shape the perception and approach of risks in the context of the digital environment, thus making it possible to analyze ways of effective coping. Symbolism, in this case, refers to the use of norms and policies that, although they appear to address complex problems, often lack practical effectiveness, creating a cycle of superficial legitimacy. In the legal and political sphere, this phenomenon takes on specific contours, especially in relation to the confrontation of risks in the digital environment and their implications for fundamental rights and socio-environmental balance, since these risks, in the sense of Beck (2002), are



mainly consequences of the symbolic functions of Science, Politics and Law that allow the materialization of risks due to bad practices arising from surveillance capitalism, as covered in Kobe et al. (2024).

In this sense, Ferreira (2016, p. 136-143) details three symbolic functions that interconnect Science, Politics and Law in the construction of an organized irresponsibility: a) symbolic function of science, which breaks scientific neutrality by producing biased knowledge that normalizes risks; b) symbolic function of politics, which adopts government measures that are ineffective or deliberately incapable of achieving its objectives; and c) symbolic function of the Law, which creates legal norms aimed at legitimizing the failures of the other two instances, completing a vicious cycle that perpetuates the normalization of risks through organized irresponsibility.

In the digital environment, these symbolic functions can be clearly observed. Science, represented by the evolution of ICTs, often operates under the discourse of neutrality, promoting technological advances without adequately addressing their negative impacts, such as the abusive use of personal data or hyperconnection that often violates the right to privacy. In turn, politics responds with legislation or programs that often lack technical robustness or effective enforcement, such as the partial implementation of data protection regulations, resulting in gaps that exacerbate digital risks. Finally, the Law, closely linked to political practices, legitimizes these practices, either through normative omissions, or by creating insufficient rules to contain abuses in the digital environment, leaving loopholes for excessive economic exploitation and structural imbalances, or by pronouncing, in the judicial sphere, decisions that prejudge the right of the injured parties (Efing, 2011), often under inopportune discourse, such as predatory litigation.

In view of this panorama, it is imperative to highlight that Beck (2002, p. 123) observes that the contemporary risk society transfers to individuals the responsibility for decisions made without adequate knowledge of their consequences. This phenomenon is amplified in the digital environment, where the risks associated with the use of data are often invisible to ordinary users, who depend on experts to interpret them. This deprivation of essential information perpetuates a culture of technological fatalism, in which decisions seem inevitable and consequences uncontrollable.

However, confronting this symbolism requires more than simple normative reforms, so that Beck (2002, p. 110) suggests overcoming technological fatalism and the abstraction of risks through the creation of new forms of organization that promote independence and transparency between science, politics, law and society. He defends an expansion of the



public sphere and a democratic debate based on scientific and informed arguments, capable of separating what is legitimate from what is symbolic and ineffective.

In the digital environment, this implies articulating public policies that transcend symbolism and promote concrete measures, such as effective inspection of data collection and use practices, digital education of consumers, and strict accountability of economic agents that unbalance the system. Thus, from a legal point of view, the dialogue of sources presents itself as an indispensable tool, allowing the integration of regulations such as the CDC, the LGPD and the PNMA, harmonizing their provisions and enhancing their application in the face of digital risks.

In this scenario, overcoming symbolic functions in Law and Politics is essential to build a balanced digital environment, where economic and technological interests are compatible with the protection of fundamental rights and sustainability. For this, it is necessary that society, the State and the productive sectors take an active role in the formulation of innovative solutions, committed not only to the appearance of protection, but to their effectiveness in facing the challenges of cyberspace.

Social participation is fundamental to deliberate on the direction of a society, including in terms of risk prevention and ways to deal with such problems. However, in order to make deliberations of this order feasible, it is necessary to have the contribution of the scientific community, including the legal community, which, in turn, must also respect internal dialectics to issue unbiased positions. Thus, the role of the Law is indispensable to regulate the deliberations and provide a form of conflict resolution, requiring more effective means to solve the problems, which can be provided based on the dialogue of the sources.

THE ROLE OF THE DIALOGUE OF SOURCES IN ADDRESSING DIGITAL RISKS INTEGRATION OF LEGAL NORMS

The integration of legal norms represents an essential element for facing the risks that emerge in the digital environment. The complexity of this ecosystem, characterized by immateriality and fluidity, requires a normative approach capable of transcending the boundaries of specific legislation, articulating several legal diplomas in a harmonious way, since, without prejudice to other applicable legal relationships, the main relationships observed, for the purposes of this article, are both of a consumerist nature, of a data subject, and of a diffuse right to a healthy environment. In this sense, the dialogue of sources, as conceived by Claudia Lima Marques (2003, p. 6-11), offers a robust theoretical basis for integrating different regulations, allowing a more efficient and coherent application of principles and rules that affect digital relations.



In the context of the digital environment, as mentioned, three regulations stand out for their relevance: the CDC, the LGPD and the PNMA. The interaction between these laws is essential to build a legal system that offers effective protection for both consumer rights and environmental balance, including in its digital dimension.

The integration between the CDC and the LGPD is a clear example of the possibility of normative dialogue in facing digital risks. The CDC, as a legal framework that protects the most vulnerable party in consumer relations, can complement the LGPD in the protection of personal data (De Oliveira & Freitas, 2021. p. 5-8). The LGPD, in turn, reinforces the right to clear and accessible information, already provided for in the CDC, expanding its application in the digital context by establishing specific rules for data processing. This complementarity is evidenced in article 7 of the CDC, which provides for the possibility for consumers to benefit from other legislation that is more favorable to them, ensuring greater protection for data subjects in situations of informational imbalance.

In addition, the concepts of vulnerability and objective good faith, central to the CDC, find correspondence in the provisions of the LGPD, which aim to ensure the responsible and proportional use of personal data. The harmonization of these instruments allows, for example, to hold accountable agents who, by processing data negligently or abusively, simultaneously violate consumer rights and data protection principles (De Oliveira & Freitas, 2021. p. 8).

Nevertheless, it is also seen that the National Environmental Policy (Law 6.938/1981) presents itself as another norm that can be integrated into the digital context, especially by recognizing the environment as a diffuse good that encompasses not only physical aspects, but also immaterial dimensions, such as the digital environment. This conception expands the application of environmental principles to cyberspace, allowing the LGPD and the PNMA to act jointly to ensure a balanced and sustainable digital environment, and may also make use of effective accountability institutes such as the duty of full reparation provided for by the CDC in its article 6, item VI.

The principle of environmental preservation, central to the PNMA, can be adapted to the digital context to support the need for mechanisms that anticipate and mitigate risks associated with data processing. Likewise, the polluter-pays principle, widely applied in cases of environmental damage, can be transposed to hold economically responsible the agents who unbalance the digital ecosystem through abusive or illegal practices, such as non-compliance with the duty of data protection (articles 6, 9, 11, 33, 46, 50 and others of the LGPD) which, in more serious cases such as data leakage, it may give rise to collective compensation for damages, in addition to the parties directly involved in the relationship,



under the terms of article 17 of the CDC and Special Appeals No. 2124701-MG and No. 2.005.977-RS, so that the simultaneous legal relationships, arising from sources such as LGPD, CDC and PNMA, allow for the reconciliation and compatibility of their normative provisions so that the damage is repaired both at the individual level (LGPD), and in the collective (CDC), at the same time that it is possible to demand the solution of the cause of the problem, through impositions of obligations that seek to reestablish the environmental balance in cyberspace (PNMA).

However, the integration of legal norms is not limited to the cumulative application of legislation; it requires the articulation of principles and values underlying these norms. Ecological balance, essential to Environmental Law, can be incorporated into Digital Law as a guiding principle for the preservation of the digital environment. Similarly, the dignity of the human person, a constitutional commandment that also makes up the core of the CDC and the LGPD, reinforces the need to protect fundamental rights in the digital environment, such as privacy, security, and access to information. Such integration, in addition to ensuring greater coherence to the legal system, promotes a systemic approach, recognizing that the problems of the digital environment are not isolated, but interdependent, requiring comprehensive and interdisciplinary solutions, since complex problems, arising from complex systems, also demand complex solutions (Capra, 2004, p. 14-20).

However, despite the advantages of this integration, there are inevitable challenges, such as normative fragmentation and the resistance of economic and institutional actors, which is why overcoming these barriers requires coordinated efforts between the Legislative, Executive and Judiciary Branches, in addition to the active participation of civil society and the committed productive sectors. Therefore, the integration of legal norms to face the risks of the digital environment demonstrates that Law, by articulating different normative microsystems, can offer more complete and effective responses to the challenges of the digital age, while this approach not only strengthens the protection of rights, but also contributes to the construction of a fairer digital environment. balanced and sustainable, for the benefit of current and future generations.

DIGITAL DEMOCRACY AND SOCIAL PARTICIPATION

Furthermore, it is observed that, combined with the need for dialogue between sources, democracy and social participation emerge as one of the fundamental pillars to face the challenges and risks associated with the digital environment since, in a context marked by hyperconnection and the growing influence of ICTs, the expansion of spaces for deliberation and the strengthening of digital citizenship become essential to promote a more



inclusive governance, transparent and effective in cyberspace, seeking to clarify the risks, their extent and discuss means of solution, especially within the legal community. In this sense, concepts such as cyberdemocracy, formulated by Pierre Lévy (2002, p. 31-32), offer a relevant theoretical basis for understanding the articulation between technology and democracy, as instruments of emancipation and collective intelligence.

Lévy (2002) defines cyberdemocracy as a modern extension of democratic practice, in which the digital environment acts as a diffuser of ideas, knowledge and debates, creating a "planetary metatext" that transcends physical and institutional limitations. This digital environment, characterized by the deterritorialization of interactions, enhances global cooperation and expands the space for citizen participation. However, the effectiveness of this digital democracy requires the strengthening of moral reciprocity and the recognition of competences among the participants, essential elements for the formation of a truly autonomous and plural public opinion, and the Law, by integrating its sources, can assist in the construction of these rules that govern this space. According to Lévy, cybernetics, in the informational context, is redefined as a foundation for citizenship, by demanding an inclusive communication environment accessible to all. This environment favors democratic debate and the deliberation of ideas. With the emergence of cyberspace supported by ICTs, this communicational flow reaches a global scale, allowing democracy to overcome physical limitations and become more fluid and deterritorialized, enabling information and decisions to be within the reach of all virtual communities (Souza, 2024, p. 172-175). Thus, cyberdemocracy is described by Lévy (2010, p. 135) as a space characterized by free interaction and cooperation, enabling a truly participatory democratic practice, which is corroborated by Han (2022, p. 47-53).

In this context, ICTs play a central role in democratizing access to information and creating more accessible communication channels. Tools such as digital platforms, social networks, and *Blockchain technologies*, for example, offer unprecedented possibilities for the exercise of political and social rights. A practical example of this is shown in the application of *Blockchain* in voting systems, which ensure greater transparency and security in electoral processes, as discussed by Souza, Nora, and Kobe (2024). However, the use of these technologies also presents challenges, such as the spread of disinformation, algorithmic manipulation, and the deepening of digital inequalities. For digital democracy, as a means of combating risks, to be effective, it is necessary to overcome these obstacles through public policies aimed at digital inclusion, technological education and responsible regulation of platforms, once again evidencing the essential role of Law in the legislative structuring that encourages, or obliges, these practices.



Social participation in the digital environment goes beyond mere access to information, implying the active involvement of citizens, exercising conscious consumption (Efing, 2016), in the formulation and deliberation of public policies that impact both the digital environment and society as a whole. Beck (2002, p. 110) asserts that, in a society of risk, the expansion of the public sphere and the redistribution of decision-making power among different actors are fundamental to overcome technological fatalism and promote a more responsible and democratic governance. In the context of the digital environment, this participation should be guided by the protection of fundamental rights, such as privacy (with a special focus on the impact of new technologies, as highlighted by Misugi et al. 2016), freedom of expression, and equitable access to technology. The articulation between these rights, as provided for in the Consumer Protection Code and the General Data Protection Law, reinforces the need for a constant dialogue between norms and values that guarantee the dignity and security of individuals in cyberspace.

Cyberdemocracy also presents itself as a means of promoting sustainability in the digital environment, enabling public debate on the impacts of ICTs and the inappropriate treatment of data that causes environmental imbalance, encouraging the creation of collaborative solutions to problems such as excessive data exploitation and informational imbalance. In addition, by integrating different voices and perspectives, digital democracy contributes to the formulation of fairer and more inclusive policies, which consider both individual and collective interests. In this context, education for digital citizenship is indispensable, insofar as, only through the development of critical and technological skills will it be possible to strengthen social participation and ensure that technological advances are directed to the common good, being the combination of an informed civil society and a harmonious normative environment, supported by the dialogue of sources, one of the bases for an effective and sustainable cyberdemocracy that can protect the digital environment.

Thus, digital democracy and social participation, combined with the full dialogue of normative sources, are crucial elements for facing the risks and challenges of the digital environment, justified by the fact that the expansion of the space for deliberation and integration of different perspectives promote not only the governance of cyberspace, but also the protection of fundamental rights and the strengthening of citizenship. both in the dimension of conscious consumption (Efing, 2016), of the data subject, and in the holder of the diffuse right to a healthy environment. However, for this potentiality to materialize, it is necessary to overcome the structural and symbolic barriers that limit digital inclusion and the transparency of democratic processes, seeking to ensure that digital democracy is not



only a reflection of the information society, but an engine for its ethical and sustainable transformation.

PROPOSALS FOR POSSIBLE IMPROVEMENTS IN PUBLIC POLICIES

It has been observed so far that the complexity of legal relationships in the digital environment requires a significant effort to harmonize specific legislations, promoting a normative approach that integrates different legal diplomas. In this scenario, the dialogue of sources plays a fundamental role in articulating rules such as the CDC, the LGPD and the PNMA, aiming at the creation of a more cohesive and efficient legal system. Miranda (2014, p. 182-187) points out that the Brazilian normative evolution is linked to the need to reconcile economic, social and environmental interests, requiring, for this, measures that strengthen the articulation between the Legislative, Executive and Judiciary branches.

In this context, it is proposed the adoption of complementary legislation that explains the interactions between the different legal diplomas, reducing normative conflicts and ensuring greater coherence in the confrontation of digital problems, even reducing any ambiguities during the application of normative commands by the Executive and Legislative Branches. In addition, the creation of interinstitutional commissions involving the National Data Protection Authority (ANPD), the Ministry of the Environment, and the National Consumer Secretariat (Senacon) can be an effective strategy to monitor abusive practices in the digital environment. Finally, it is suggested to review and extend the statute of limitations for environmental and digital liability actions, ensuring that victims of harmful practices have greater reach and access to justice.

The protection of the digital environment, however, cannot be limited to legal instruments; it must be complemented by public policies aimed at social and technological inclusion. According to Miranda (2014, p. 187-193), it is crucial to align consumer rights with the demands of sustainability and innovation, since awareness and education play central roles in strengthening digital citizenship. To this end, it is proposed the development of educational programs that enable consumers to understand the risks associated with data processing, promoting a conscious use of digital technologies, being able to use cyberspace itself, which currently has a robust streaming culture and social networks that exponentially disseminate information, and this diffusing power should be used to propagate consumer and data subject education.

In addition, another essential point is the formulation of policies that encourage transparent and sustainable business practices in the use of data, linking, for example, tax incentives to the adoption of measures that minimize environmental impacts resulting from



digital operations, complemented by information campaigns, as mentioned above, aimed at the general population, using digital and traditional platforms, can disseminate knowledge about consumer rights in the digital environment, especially with regard to privacy, security, and redress mechanisms in cases of imbalances in the digital environment.

As highlighted by Miranda (2014, p. 193-194), overcoming the culture of normative and symbolic negligence is a challenge that demands the implementation of public policies based on cooperation between economic actors, civil society and the State. This integrated approach not only strengthens the protection of fundamental rights in the digital environment, but also contributes to the preservation of human dignity and socio-environmental balance in an increasingly digitized and complex context.

CONCLUSION

The present study highlighted the challenges imposed by the digital environment and the contemporary risk society, highlighting the need for legal, social and political responses compatible with the complexity of this scenario. From the socio-environmentalist perspective, as pointed out by Beck, it is recognized that human action, by promoting changes that are often harmful to the environment, both natural and digital, generates significant risks that undermine not only the sustainability of the environment, but also the healthy survival of humanity. This awareness, as observed by Morin and Kern (2003, p. 64), is fundamental to recognize the human condition as a citizen of the Earth, assuming responsibilities for the preservation of a balanced and healthy environment by all those involved and, above all, those who cause the ecological imbalance.

In this context, full digital democracy and the dialogue of sources is presented as one of the crucial tools for addressing environmental imbalances. By creating an inclusive space for debate and social participation, it is possible for experts and citizens (consumers, data subjects, and holders of diffuse rights) to identify problems in cyberspace and propose solutions that integrate technical knowledge and varied perspectives. Thus, the digital environment can be converted into an ally in the construction of more sustainable and transparent practices, overcoming the symbolic functions of science, politics, and law, which often perpetuate organized irresponsibility and normative ineffectiveness.

In turn, the dialogue of sources was identified as an essential element for overcoming the challenges of the digital environment. The normative articulation between the Consumer Protection Code (CDC), the General Data Protection Law (LGPD) and the National Environmental Policy (PNMA) expands the protection of citizens' rights and allows for an integrated approach, capable of holding accountable agents who adopt harmful



practices. Some emblematic cases, such as Special Appeals No. 2124701-MG and No. 2.005.977-RS, demonstrate the applicability of this dialogue, by showing that consumer protection by equivalence can be extended to digital disasters, such as data leaks, which generate risks similar to environmental disasters in cyberspace.

Thus, inspired by Capra (2004, p. 14-20), it is observed that problems related to the digital environment must be understood as interdependent and systemic, requiring equally complex solutions. Measures such as the extension of the statute of limitations, the strengthening of the joint action of public agencies, such as the ANPD, and the promotion of digital education of consumers/data subjects were identified as concrete strategies to contribute to the socio-environmental balance in this environment.

Finally, it is concluded that the protection of the digital environment, as an extension of the natural environment, cannot be achieved through fragmented approaches. It is necessary to foster an integrated and sophisticated legal system, as well as a robust social engagement, capable of facing the globalized digital risks that characterize contemporary society. Only through an effective dialogue between norms, institutions and participatory democracy will it be possible to build a sustainable and fair future, both physically and digitally.



REFERENCES

1. Alves, F. G., Sousa, P. H. da M. R., & do Rêgo, D. N. (2024). Publicidade parasitária e possível tutela do consumidor a partir da utilização de inteligência artificial pelas plataformas de mídia social. *Revista Jurídica Cesumar-Mestrado*, 24(1), 287–298.
2. Beck, U. (2002). *La sociedad del riesgo global*. Siglo Veintiuno.
3. Campos, R. (2022). *Metamorfose do direito global: sobre a interação entre direito, tempo e tecnologia*. Editora Contracorrente.
4. Capra, F. (2004). *A teia da vida*. Cultrix.
5. Capra, F. (2006). *As conexões ocultas*. Cultrix.
6. Castells, M. (2003). *A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade*. Zahar.
7. Cavedon, R., Ferreira, H. S., & Freitas, C. O. de A. (2015). O meio ambiente digital sob a ótica da Teoria da Sociedade de Risco.
8. Coutinho, R. S. (2014). O meio ambiente digital e a tutela dos bens culturais. *Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação*, 1(1), 221–244. <https://doi.org/10.37594/rbmads.v1i1.223>
9. Davenport, T. H. (1998). *Ecologia da informação – porque só a tecnologia não basta para o sucesso na era da informação* (B. Siqueira Abrão, Trans.). Futura.
10. De Oliveira, D. H. Z., & Freitas, C. O. de A. (2021). A responsabilidade civil do fornecedor quanto aos dados pessoais do consumidor: Diálogo das fontes entre CDC e LGPD. *Revista de Direito do Consumidor*, 138, 225–242.
11. Doneda, D. (2011). A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJLL]*, 12(2), 91–108.
12. Efing, A. C., & Geromini, F. P. (2016). Crise ecológica e sociedade de consumo. *Revista Direito Ambiental e Sociedade*, 6(2).
13. Efing, A. C., Gibran, F. M., & Blauth, F. N. L. (2011). A proteção jurídica do consumidor enquanto direito fundamental e sua efetividade diante de empecilhos jurisprudenciais: o enunciado 381 do STJ. *Revista Brasileira de Direitos Fundamentais & Justiça*, 5(17), 207–226.
14. Ferreira, H. S. (2016). A dimensão ambiental da teoria da sociedade de risco. In H. S. Ferreira & C. O. de A. Freitas (Orgs.), *Direito Socioambiental e Sustentabilidade: Estados, Sociedades e Meio Ambiente* (pp. 108–158). Letra da Lei.
15. Freitas, C. O. de A. (2022). Riscos e proteção de dados pessoais. *Revista Rede de Direito Digital, Intelectual & Sociedade*, 2(4), 1–319.
16. Gartner. (2024). *Information Technology Glossary*. Available at <https://www.gartner.com/en/information-technology/glossary/digitization>; accessed on November 20, 2024.



17. Gleick, J. (1987). *Chaos-making a new science*. Viking.
18. Han, B.-C. (2022). *Infocracia: Digitalização e a crise da democracia* (G. S. Philipson, Trans.). Vozes.
19. Hoffmann-Riem, W. (2021). *Teoria Geral do Direito Digital: Transformação digital; desafios para o direito* (I. Fuhrmann, Trans.). Forense.
20. Kobe, W. R., Ferreira, H. S., & Freitas, C. O. de A. (2024). Distopia cibernética e meio ambiente digital. *Prisma Jurídico*, 23(2), 315–335. <https://doi.org/10.5585/2024.26656>. Available at <https://periodicos.uninove.br/prisma/article/view/26656>. Accessed on December 18, 2024.
21. Koskenniemi, M. (Coord.) apud Campos, R. (2022). *Metamorfose do direito global: sobre a interação entre direito, tempo e tecnologia*. Editora Contracorrente.
22. Lévy, P. (2010). *Cibercultura* (3rd ed.). Ed. 34.
23. Lévy, P. (2002). *Ciberdemocracia*. Instituto Piaget.
24. Lévy, P. (2008). O ciberespaço como um passo metaevolutivo. *Revista FAMECOS*, 7(13), 59–67.
25. Marques, C. L. (2003). Diálogo entre o código de defesa do consumidor e o novo código civil – do “diálogo das fontes” no combate às cláusulas abusivas. *Revista de Direito do Consumidor*, 45, 71–99.
26. Miranda, J. E. de. (2014). Evolução, regime jurídico, problemas e perspectivas do direito do consumidor no Brasil. In J. L. Tomillo Urbina (Ed.), *La protección jurídica de los consumidores en el espacio euroamericano* (pp. 61–80). Editorial Comares.
27. Misugi, G., de Almendra Freitas, C. O., & Efig, A. C. (2016). Releitura da privacidade diante das novas tecnologias: realidade aumentada, reconhecimento facial e internet das coisas. *Revista Jurídica Cesumar-Mestrado*, 16(2), 427–453.
28. Morin, E., & Kern, A. B. (2003). *Terra-Pátria*. Sulina.
29. Presse, F. (2014, June 29). Em experimento secreto, Facebook manipula emoções de usuários. *Globo*. Available at <https://g1.globo.com/tecnologia/noticia/2014/06/em-experimento-secreto-facebook-manipula-emocoes-de-usuarios.html> accessed on November 20, 2024.
30. Sarlet, I. W. (2022). Fundamentos constitucionais: O direito fundamental à proteção de dados. In D. Doneda et al. (Eds.), *Tratado de proteção de dados pessoais* (pp. 21–60). Forense.
31. Souza, L. R. de. (2024). *A ciberdemocracia cooperativa como alternativa às assembleias gerais para o exercício da gestão democrática de sociedades cooperativas*. Pontifícia Universidade Católica do Paraná.



32. Souza, L. R. de, Nora, H. D., & Kobe, W. R. (2024). Aspectos de sustentabilidade acerca do voto eletrônico baseado em blockchain em assembleias online. *Revista Políticas Públicas & Cidades*, 13(2), e1023. <https://doi.org/10.23900/2359-1552v13n2-214-2024>. Available at <https://journalppc.com/RPPC/article/view/1023>. Accessed on November 20, 2024.
33. Zuboff, S. (2020). *A era do capitalismo de vigilância: A luta por um futuro humano na nova fronteira do poder* (G. Schlesinger, Trans.). Intrínseca.