CONSUMER PERSONAL DATA PROTECTION IN BRAZIL AND THE STATE OF CALIFORNIA (USA): A CRITICAL ANALYSIS OF THE BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD) AND CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

Newton De Lucca *
Guilherme Magalhães Martins **
Renata Capriolli Zocatelli Queiroz ***

Abstract: The issue of this work focuses on the critical analysis of the relevance of consumer personal data protection in the information society. The objective is to explain the relevance of the topic in light of the Brazilian General Data Protection Law and the California Consumer Privacy Act in the United States, in a micro-comparative approach. The literature review method was used, based on the theoretical-scientific construction through a comparison of the Brazilian and Californian legislation. To better understand the importance of protecting personal data today, the article discusses the global context of the knowledge society, the changes it has brought about in consumer relations, and then analyzes the Brazilian General Data Protection Law and the California Consumer Privacy Act. After studying both laws, it concludes that, considering the experience of the State of California and the growth of e-commerce in the country, it is up to Brazil to regulate the matter of protecting the consumer's personal data.

Keywords: personal data; consumer; specific legislation.

INTRODUCTION

The popularization of the internet has transformed social relationships, directly impacting the way individuals act in the family, professional, political, commercial and other contexts. The growth of the e-commerce market has substantially changed the consumer buying behavior and sales of companies, generating a great challenge for everyone to adapt to the new changes.

* Ph.D, University of São Paulo (USP); Full Professor, University of São Paulo (USP). Email: newtonde@uol.com.br / ORCID iD: https://orcid.org/0000-0002-9393-5512
** Ph.D, University of the State of Rio de Janeiro (UERJ); Associate Professor, Federal University of Rio de Janeiro (UFRJ). Email: gmartins@mprj.mp.br / ORCID iD: https://orcid.org/0000-0003-3082-656X
*** Ph.D, University of São Paulo (USP); Professor, Londrina University. Email: renataczqueiroz@gmail.com / ORCID iD: https://orcid.org/0000-0002-6348-751X
The problem of this work focuses on the critical analysis of the relevance of the protection of consumer personal data in the information society. The objective is to explain the relevance of the theme in light of the General Data Protection Law in Brazil and the California Consumer Privacy Act in the United States, in a micro-comparative approach.

The first part of this article will address the global context of the knowledge society, the changes it has brought about in consumption relationships and the need for protection of consumer personal data in the face of its intense exposure in the market.

In this context, the protection of the right to privacy and the protection of personal data become increasingly expressive. Thus, the second part of this article will address the Brazilian legislation on the subject, with the focus on the General Data Protection Law and the Consumer Defense Code.

In 2018, in the same year of publication of the LGPD, the State of California (USA) published the Consumer Privacy Act (CCPA), with the objective of offering consumers more control over the personal information that companies collect about them. Additionally, the respective regulations provide the necessary guidance on the implementation of the law. Thus, the Consumer Privacy Act (CCPA) and the fundamental rights protected by the legislation will be addressed.

I. THE CONSUMER AND THE INFORMATION SOCIETY

The use of information and communication technologies, amplified by the popularization of the internet, characterizes the Knowledge Society. Pierre Lévy explains that:

"[...] intelligence or cognition is the result of complex networks where large numbers of human, biological and technical actors interact. It's not 'me' who is intelligent, but 'me' with a human group of which I am a member, with my language, with all a heritage of intellectual methods and technologies (among which, the use of writing)."

For the author, the emergence of the computer and the network that interconnects the entire planet was a great acquisition for humanity, since cyberspace, when it promotes interaction among users, causes them to acquire and share knowledge.

The emergence of the expression "information society" in Europe is

---

2 According to José de Oliveira Ascensão, the information society encompasses elements related to computer programs, integrated circuits, electronic databases and the use of works by computer. The universal base of all these phenomena is digitization. It is this
attributed to the 1980 international conference, where the European Economic Community brought together scholars to evaluate the future of a new society thus named, given the regulation of the freedom of circulation of services and measures for access to goods and services by the Member States. The expression TIC - information and communication technologies was then used for the first time.\textsuperscript{3}

However, an embryonic view of the matter could be seen earlier in the 1970s in Japan, when Yoneji Masuda, in his studies, sought the realization of a society that brought a general and flourishing state of human intellectual creativity, instead of a material consumption. The author points out that in 1972, a Japanese non-profit organization, the Japan Computer Usage Development Institute, presented to the government the "Plan for the Information Society" - a national objective towards the year 2000. The author reports having been appointed manager of this ambitious national plan, and being attributed the first use of the expression ("information society") in the English language.\textsuperscript{4}

The popularization of the use of the internet brought many gains, but also risks. Regarding the subject, Leonardo Parentoni\textsuperscript{5} explains that the technological development of the last decades, provided by the peak of the internet, brought to society a multitude of problems and questions related to privacy. In this sense, Ulrich Beck states: "the old industrial society, based on the distribution of goods, was being replaced by a new risk society, structured in the distribution of evil".\textsuperscript{6}

Technologies imply a loss in the ability to control one's own identity, to make choices that concern freedom, a fundamental aspect of human dignity, and informational self-determination, considering the exposure resulting from the architecture of the Internet. Doctrine uses the expression "glass consumers" in reference to the human person on the Internet, so that others


know so much about us that they can see through us. Our daily lives are recorded, analyzed, and monitored in countless non-perceptible or even consented ways.\(^7\)

Despite the changes caused by the popularization of the internet in consumer relationships, it becomes appropriate to recall the concept of commercial law, in the words of the author Cesare Vivante: "Commercial law constitutes that part of private law that has, primarily, as its object to regulate the circulation of goods between those who produce them and those who consume them".\(^8\)

Since the internet is a tool that brings physical and legal people together, it allows the entrepreneur to showcase his products and services to consumers. Thus, considering the low cost of online operation, e-commerce has become an attraction to companies, especially when the entrepreneur seeks to expand his business.

Regarding the impacts of the internet on commercial law, Tarcísio Teixeira\(^9\) explains that in the beginning, commerce developed through fairs, e-commerce. For the author, e-commerce represents the future of commerce, since there are countless business opportunities spread across the network. In the transition from automatic machines to computer science, especially in the field of consumer relations, the so-called unweighted contract stands out, through an artificial creation of needs, appearing as the apex and protagonist of the dissolution of the voluntarist system.\(^10\)

In consumer relations, considering the often existing unequal relationship between the consumer and the supplier, risks are amplified. Zygmunt Bauman\(^11\) states that in a consumer society, it is not possible to become a subject without first becoming a commodity, since "the subjectivity of the subject, and most of what that subjectivity enables the subject to achieve, is concentrated in an endless effort to become and remain a saleable commodity". Regarding the vulnerability of the consumer, it is worth mentioning that it is even more glaring in e-commerce, and can be physical, technical, legal or informational.\(^12\)

---


\(^12\) Regarding the types of vulnerability, Tarcísio Teixeira states that "it is worth explaining that factual or socio-economic vulnerability occurs when there is an inferiority of the buyer in the face of the privileged or superior position of the seller, taking into account its economic size or due to the essentiality of the product, for example, if a doctor buys a car
Considering the greater vulnerability of the consumer in the electronic environment and the exposure of their data on the internet, the importance of protecting their data on the internet is emphasized. Regarding the need for personal data protection legislation with the goal of balancing the guarantee of individual liberties and rights, Selma Carloto states:

"The technological advances of recent years, with new information technologies, have come to permanently alter the world around us and brought the need for personal data protection legislation that seeks the balance between the guarantee of individual liberties and rights, and which translates into the preservation of the privacy of private life and the freedom of circulation of personal information."\(^\text{13}\)

Therefore, considering the current moment of society, the transformations proposed by the information society in commercial law and the great exposure of consumer data on the internet, the next chapter will address the General Data Protection Law and Consumer Law in Brazil.

II. THE GENERAL LAW FOR THE PROTECTION OF PERSONAL DATA AND CONSUMER RIGHTS - BRAZIL

The protection of personal data in Brazil, before the publication of the General Data Protection Law, was already an object of protection in Brazilian legislation.\(^\text{14}\) Among these, considering the object of analysis of this research, the Consumer Defense Code\(^\text{15}\), Law 8,078 of September 11, 1990 (LGL\(\text{1990}\)\(\text{40}\)), which deals with consumer protection and provides other measures, stands out.

Before proceeding with the research with the analysis of the protection of personal data contained in the Consumer Defense Code, it is important to address what the law understands by consumer. In terms of Article 2 of the

---

\(^{13}\) Carloto, Selma, A Lei Geral de Proteção de Dados: enfoque nas relações de trabalho, 2nd ed. São Paulo: LTr, 2021, 16.

\(^{14}\) Some examples are the Federal Constitution, the Habeas Data Law, the Public Archives Law, the Civil Code, the Consumer Defense Code, the Law of Information Access, and the Internet Civil Framework.

Law, consumer is any natural or legal person who acquires or uses a product or service as the final recipient. On the concept, author Claudia Lima Marques explains:

"The final recipient is the actual and economic recipient of the product or service, whether it be a natural or legal person. So, according to this teleological interpretation, it is not enough to be the actual recipient of the product, to take it out of the production chain, take it to the office or home, it is necessary to be the economic final recipient of the good, not to buy it for resale, not to buy it for professional use, as the good would be a production instrument whose price will be included in the final price of the professional who acquired it. In this case there would be no required "final destination" of the product or service."\(^{16}\)

Regarding this interpretation, it is worth highlighting that the Law, in its Article 29, equates all determinable or not, exposed to the practices it provides for, to the consumer. In other words, it did not limit its application to the final recipient of the product or service, but also to the protection of the consumer by analogy, guaranteeing the incidence of the Consumer Defense Code regardless of the existence of the prior contractual relationship between the parties.

For there to be a consumer relationship, it becomes necessary for the existence of the supplier, which, in the terms of Article 3 of the law, is any natural or legal person, public or private, national or foreign, as well as impersonal entities, who carry out the activity of production, assembly, creation, construction, transformation, import, export, distribution or marketing of products or provision of services.\(^{17}\)

When analyzing the Consumer Defense Code and the protection of personal data, the Section VI stands out, which deals with consumer databases and registers from Article 43. However, before entering into the content in the aforementioned article, it is necessary to first address the principles of the CDC (LGL\(1990\)\(40\)) that guide its interpretation. They are: good faith, transparency, security and full repair of damage.

Good faith is explicitly provided for in Article 4\(^a\), III\(^{18}\) of the CDC


\(^{18}\) "Art. 4º. [...] III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores".
(LGL\1990\40), and constitutes the basic principle of the Code, especially in terms of contractual relationships. Regarding the practice of good faith in forming databases, the author Rita Peixoto Ferreira Blum\(^\text{19}\) states that it must be observed in all phases of the contract, from the beginning of the contractual relationship, when the consumer's first data begins to be collected; the consumer's agreement or disagreement regarding the collection and use of the data according to its purpose must be solicited.

The principle of transparency, set forth in the caput of Article 4\(^\text{20}\), in the words of Maria Stella Gregori: “the principle of transparency is translated by the imposition on the supplier of the duty to ensure correct, clear, precise, ostensible and Portuguese information when offering or presenting their products and services”\(^\text{21}\). It can be noted that this principle is divided into the rights set forth in Article 6\(^\text{2}\), II and III, which, respectively, deal with the right to receive adequate disclosure and the right to receive clear and adequate information about different products and services, including correct specification of the quantity, characteristics, composition, quality, taxes incurred in the price and the risks presented.

With regard to security, Article 6, I, provides for the protection of life, health and safety against the risks caused by practices in the provision of products and services considered dangerous or harmful. As discussed in the first chapter, the knowledge society exposes the individual to risk, especially with the accumulation of their information in voluminous data banks. In this context, the author Rita Peixoto Ferreira Blum\(^\text{22}\) explains that

"[...] the right to security generates expectation in the consumer that their data, when provided to the supplier, will be stored adequately with information security mechanisms currently available in the market."

Finally, in the last principle listed, the comprehensive security of damages, provided for in Article 6, V\(^\text{23}\), the consumer has the right to compensation for material and moral, individual, collective and diffuse damages. The rule of civil liability provided for in the Consumer Protection


\(^{20}\)“Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios [...]."


\(^{23}\)“Art. 6º. [...] VI - a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos”.
Code (LGL\1990\40) is objective, so the consumer has the right to full compensation for damage when handling and conserving their personal data in non-compliance with the law that causes damage.

Article 43\(^{24}\) provides that the consumer will have access to information in records, files, registries and personal and consumer data stored about them, as well as about their respective sources.

As provided for in Article 43, in addition to the right to access information in records and their sources, when the record is opened, the consumer has the right to be notified in writing when not requested by them.

In relation to inconsistencies regarding the registered data, if any inaccuracy is found in the registration, it can require immediate correction within five working days. It is worth mentioning that negative information about the consumer cannot be filed for more than five years. Furthermore, the law equates databases and registration regarding consumers to a public entity.

Regarding the focus given by the wording of Art. 43, Roberto Pfeiffer states:

"Thus, the concern of Art. 43 is double. On the one hand, it preserves an instrument of protection for suppliers, which serves as a prevention against the risk of default. [...] on the other hand, however, it aims to protect the consumer's privacy, preserving it from abusive actions that the supplier or the database operator may take. The conclusion, therefore, is that the Consumer Defense Code applies indifferently to credit protection databases controlled by public or private entities."\(^{25}\)

\(^{24}\) “Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.”

“§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata corrigida, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formato acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor”.

\(^{25}\) Pfeiffer, Roberto, Práticas Abusivas, Cobrança de Dívidas e Cadastro de Consumo, in Teresa Ancona Lopez & Ruy Rosado de Aguiar Jr., eds., Contratos Empresariais, Contratos
With regard to the focus given by the wording of Art. 43, it is necessary to say that the author Rita Peixoto Ferreira Blum concludes that the article addresses in more detail the discipline of the credit protection database than that of the consumer registration:

"Considering the distinction above, it is possible to affirm that the content of Art. 43 focuses in more detail on the discipline of the credit protection database than on that of the consumer data registration. This is demonstrated by examining the last two paragraphs of the provision, in which the legislator dedicated himself to complementing the regulation of the treatment of negative credit data. The law is clearly more extensive in this matter than in the discipline of other consumer data. Consequently, in the result of the research for this thesis, doctrine and jurisprudence were obtained in a significant amount regarding Art. 43, with a focus on databases and negative credit information. It is a much larger number than the material found regarding the consumer data registration, in addition to credit information, about which only about eight decisions were found."

Despite the doctrinal discussion about the focus given by Art. 43 of the CDC (LGL 1990 40), the fact is that there was no specific law in Brazil that legislated about the protection of personal data. Thus, on August 14, 2018, influenced by the European Union's General Data Protection Regulation, the General Data Protection Law of Personal Data was published in Brazil, which regulates the treatment of personal data, including in digital media, by a natural person or by a public or private legal entity.

Regarding the relevance of the existence of this legal diploma, Newton De Lucca's advocacy experience stands out, when he recounts that several times he received foreign business groups in his office with the purpose of establishing a joint venture with Brazilian companies. At the moment when they asked him about the existence of the Brazilian personal data protection system, which was then non-existent, he reported that, despite exposing that the country had constitutional provisions foreseeing the corporification of this fundamental right, unfortunately, most of the time, the business would be abandoned due to the legal gap at the time.

It should be noted that the aim of the General Law on the Protection of Personal Data is to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person. On the subject,


Danilo Doneda writes:

"The expression data protection itself does not accurately reflect its core, as it is the result of a development process in which various interests were involved - it is not the data that is protected, but the person to whom such data refers."

The LGPD understands personal data as any information related to the identified or identifiable natural person. Regarding those involved in the data processing activity, according to article 5, paragraph V, of the LGPD, the holder is the natural person to whom the personal data that is the subject of processing refers. Regarding the concept of data processing agent, the controller and operator are understood, according to subparagraph IX of this article, which will be the subject of study in the subitems of this chapter.

With the aim of achieving its objectives, the LGPD imposes, in a practical way, rules for the processing of personal data, establishing a series of obligations for the processing of personal data in Brazil.

The LGPD considers as personal data any information related to an identified or identifiable natural person. It is guided by various principles,

---

29 “Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; [...].”
30 “Art. 5º Para os fins desta Lei, considera-se: [...] “VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; [...]”
31 “Art. 5º Para os fins desta Lei, considera-se: [...] “VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”.
32 “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
   I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
   II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
   III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
   IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
   V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
   VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
including good faith, transparency, security, and full repair of damage, provided in the CDC (LGL 1990 40), as mentioned above. Despite the LGPD, it is appropriate to highlight that, in order to take care of, implement, and enforce compliance with the legislation, the National Authority for Data Protection is created.\footnote{Brazil, Decree No. 7962, March 15, 2022, available at [www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm] accessed Feb. 1st, 2023.}

Furthermore, regarding the protection of personal data in the Brazilian legal system, it is worth mentioning Constitutional Amendment 155/2022, recently published, which included the fundamental right to the protection of personal data in the constitutional catalog of rights, through the insertion of item XII-A, in art. 5, and item XXX, in art. 22, establishing, in the latter case, the exclusive competence of the Union to legislate on the matter that is in progress in the legislature.

At the same time, regarding the regulation of consumer rights in electronic commerce, it is appropriate to mention Decree 762\footnote{“Art. 1º Este Decreto regulamenta a Lei 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico, abrangendo os seguintes aspectos: I - informações claras a respeito do produto, serviço e do fornecedor; II - atendimento facilitado ao consumidor; e III - respeito ao direito de arrependimento”}, of March 15, 2013, which regulates, albeit insufficiently, the Consumer Defense Code to deal with electronic contracting. Regarding its content, it regulates the following rights of the law: right to information, facilitated service, and right to regret\footnote{“Art. 5º Para os fins desta Lei, considera-se: [...] XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional”}, that is, it regulates nothing about the consumer’s personal data in internet shopping.

The approval of Bill 3.514/2015, approved by the Federal Senate, is urgent, which aims to regulate electronic commerce in Brazil, reducing existing asymmetries in the market and protecting security, privacy, and informational self-determination.

As defined by Professor Cláudia Lima Marques, the new visual, fluid, fast, aggressive, pseudo-individual and massified language of distance
consumer legal transactions on the Internet imposes serious challenges for private law, especially for consumer law and the good faith paradigm.\textsuperscript{36}

The principiologically option of PL 3.514 is clear in the wording of Article 3-A, which, by establishing that the rules and legal transactions should be interpreted and integrated in the most favorable way for the consumer, brings to the general provisions of the Consumer Defense Code a norm previously only located in the chapter on contractual protection (art. 47).\textsuperscript{37}

The PL 3.514/2015 deals with issues such as the basic rights of consumers (proposed amendment to Article 6 of the Consumer Defense Code (LGL\textsuperscript{1990\textsuperscript{40}})), the right to information (Article 45-B), group purchases (Article 45-C), consumer access to all business information (Article 45-C), spam (Article 45-F), the right of remorse (Article 49), administrative sanctions (Articles 56 and 59), as well as rules regarding consumer protection in international consumer contracts (Article 101).

Having made the considerations regarding the matter in Brazil, with a focus on the Consumer Defense Code (LGL\textsuperscript{1990\textsuperscript{40}}) and the LGPD, the following chapter will address the Consumer Privacy Law (CCPA) of the state of California (USA).

III. CALIFORNIA CONSUMER PRIVACY ACT (USA)

The California Consumer Privacy Act (CCPA)\textsuperscript{38}, published by the State of California in 2018, aims to offer consumers greater control over the personal information that companies collect about them.

Before addressing the rights provided in the law, it is appropriate to clarify the understanding of the concepts of consumer, business and personal information for better understanding of its applicability.

Initially, it is worth noting that the law is intended to protect the consumer and, as defined in Section 17014 of Title 18 of the California Code of Regulations and Section 1798.40\textsuperscript{39} of Title 1.81.5, consumer means an individual residing in California, regardless of identification, including any unique identifier. The law only applies to consumers residing in California,


\textsuperscript{39} A consumer is described as “a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations . . . however identified, including by any unique identifier”.
i.e., individuals residing in the state, even if they are temporarily out of the state.

With regard to the concept of business, also in the terms of Section 1798.140 of Title 1.81.5, for-profit companies doing business in California that meet any of the requirements of: (a) having an annual gross revenue of over $25 million; (b) buying, receiving or selling the personal information of 50,000 or more California residents, households or devices; and (c) obtaining 50% or more of their annual revenue from selling personal information of California residents, are subject to the obligations contained in the CCPA.

Regarding personal information, the CCPA, in the terms of Section 1798.140 of Title 1.81.5, comprehends information that identifies, relates to, describes, is reasonably capable of being associated with, or could

\[40\text{(d) "Business" means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households. (C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.".}

\[41\text{“(v) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers. (B) Any personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act ( 20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99 ). (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. (L) Sensitive personal information.".}
reasonably be linked, directly or indirectly, with a particular consumer or household. The law provides examples of what is considered personal information, some of them: geolocation data, professional information, biometrics, among others.

The CCPA, under Title 1.81.5, Section 1798.100, grants new privacy rights to California consumers, including the right to know, the right to delete, the opt-out of sale, and the non-discrimination of personal data.

Regarding the right to know, the law imposes on companies the duty to disclose to the consumer the categories and specific parts of the personal information that the company collected.42

The consumer may request from the companies the disclosure of the personal information collected, used, shared, and sold, as well as the reason for the processing of the data.

The consumer may request, free of charge and specific to the 12 months prior to the request43, (a) the categories of personal information collected, (b) specific parts of personal information collected, (c) the categories of sources from which the company collected personal information, (d) the purposes for which the company uses personal information, (e) the categories of third parties with whom the company shares personal information, and (f) the categories of information that the company sells or discloses to third parties.

Regarding the right to delete44, the consumer may request that the companies delete the collected personal information and also inform their service providers to do the same. Regarding this right, it is worth noting that the law has exceptions45, which allow companies to maintain the personal

42 “(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to subparagraph (B) of paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer, provided that a business shall be deemed to be in compliance with paragraphs (1) to (4), inclusive, of subdivision (a) to the extent that the categories of information and the business or commercial purpose for collecting, selling, or sharing personal information it would be required to disclose to the consumer pursuant to paragraphs (1) to (4), inclusive, of subdivision (a) is the same as the information it has disclosed pursuant to paragraphs (1) to (4), inclusive, of subdivision (c)”.

43 “(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following: (1) The categories of personal information it has collected about that consumer. (2) The categories of sources from which the personal information is collected. (3) The business or commercial purpose for collecting, selling, or sharing personal information. (4) The categories of third parties to whom the business discloses personal information. (5) The specific pieces of personal information it has collected about that consumer”.

44 “(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer”.

45 “(d) A business, or a service provider or contractor acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably
information of consumers.

Regarding the right of not selling option\(^\text{46}\), the consumer may request that companies stop selling their personal information, and its commercialization is expressly prohibited after the consumer's request. In these cases, the company is required to wait for a minimum period of 12 months\(^\text{47}\) before requesting the consumer's authorization to commercialize their personal information again.

The right to non-discrimination\(^\text{48}\) prevents companies from denying necessary for the business, service provider, or contractor to maintain the consumer's personal information in order to: (1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer. (2) Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes. (3) Debug to identify and repair errors that impair existing intended functionality. (4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law. (5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code. (6) Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent. (7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information. (8) Comply with a legal obligation\(^\text{46}\).

\(^{46}\) "(a) A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing. (b) A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the "right to opt-out" of the sale or sharing of their personal information".

\(^{47}\) "(3) A company can enroll a consumer in a financial incentive program only if the consumer gives the company prior consent according to Section 1798.130, which clearly describes the material terms of the financial incentive program and which can be revoked by the consumer at any time. If a consumer refuses to provide opt-in consent, the company must wait at least 12 months before requesting the consumer to provide opt-in consent again, or as prescribed by regulations adopted according to Section 1798.185".

\(^{48}\) "(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by: (A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties. (C) Providing a different level or quality of goods or services to the consumer. (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. (E) Retaliating against an employee, applicant
goods or services, charging different prices, or providing different levels or quality of goods or services if the consumer exercises the rights provided by the CCPA.

In cases where personal information is necessary for the provision of goods and services and the consumer refuses to provide their personal information to the company or requests its deletion, the company may not be able to complete the transaction. The law allows companies to offer promotions, discounts, and other offers in exchange for collecting, maintaining, or selling their personal information.49

In order to enforce the CCPA, the law creates the California Privacy Protection Agency, which has been invested with full administrative power, authority, and jurisdiction to implement and enforce the CPPA.50

The law went into effect on July 1, 2020, and since then, the Office of the Attorney General, responsible for monitoring compliance with the legislation, has begun sending notifications to companies that allegedly do not comply with the law. From the receipt of the notification, the company has thirty days to promote compliance.51
CONCLUSION

The popularization of internet use has transformed commercial relationships, bringing countless benefits, but also risks. The data-driven economy has directly impacted consumer relationships, on which the right to protect personal data should be given greater attention.

With regard to protecting the personal data of consumers in Brazil, as demonstrated by the article, the Consumer Defense Code provides, in its article 43, and in the principles present in the law, protective matter regarding the consumer's personal data. However, it was only with the LGPD in 2018 that the Brazilian legal system began to specifically protect personal data in the country. Additionally, in 2022, through the Constitutional Amendment 155/2022, it was elevated to the category of a fundamental right in Brazil.

In 2018, the State of California - USA also published the Consumer Privacy Law, with the aim of ensuring greater control over personal data for consumers residing in the State of California. Among the rights provided by the CCPA, the article emphasized the right to: know, delete, no-sale option and non-discrimination regarding the treated personal data.

Therefore, considering the experience of the State of California, the growth of e-commerce in Brazil, and the foundation of the protection of consumer rights, provided in article 2 of the LGPD, it is appropriate in Brazil to regulate the protection of consumer personal data.

The National Authority for Data Protection, the public administration body responsible for overseeing, implementing, and enforcing this law, under Article 55, has the authority to develop guidelines for the National Policy for the Protection of Personal Data and Privacy. In other words, the ANPD can develop specific guidelines for the protection of personal data in consumer relationships.

It is known of the current challenges faced by the ANPD, such as the numerous matters to be regulated, the small size of the Authority's staff, among others. However, it is emphasized the relevance of the matter to be regulated and the possibility of counting on the support of other bodies for studies and the elaboration of guidelines, such as the National Consumer Secretariat - SENACON, with which, in fact, the ANPD already has a technical cooperation agreement\(^{52}\) signed and a published orientation guide.\(^{53}\)


\(^{53}\) GOV. Autoridade Nacional de Protecção de Dados e Secretaria Nacional do Consumidor, "GOV. National Authority for Data Protection and National Consumer
REFERENCES


GOV. Autoridade Nacional de Proteção de Dados e Secretaria Nacional do Consumidor, "GOV. National Authority for Data Protection and National Consumer Secretariat Launch Guide "How to Protect Your Personal Data",


Vivante, Cesare, Elementi di diritto commerciale. Milan: Ulrico Hoepli,
1936.

* * *

Newton De Lucca
Doctor, Master, and Free-Docent, Adjunct and Full Professor at the Faculty of Law of the University of São Paulo, where he teaches in both undergraduate and graduate courses. He is an Emeritus Professor of the Permanent Stricto Sensu Graduate Corps of UNINOVE and also a member of the Paulista Academy of Magistrates, the Paulista Academy of Law, and the Paulista Academy of Legal Letters. He is the Vice President of the Latin American Institute of Private Law and Vice President of the Advancement Institute of Data Protection - IAPD and a Federal Judge of the 3rd Region TRF (President in the 2012/2014 biennium).
Email: newtonde@uol.com.br
ORCID iD: https://orcid.org/0000-0002-9393-5512

Guilherme Magalhães Martins
Post-doctor in Commercial Law at the Faculty of Law of USP. He is an associate professor of Civil Law at the National Faculty of Law - UFRJ. He is a permanent professor of the Doctorate in Rights, Institutions and Businesses at the Federal University of Fluminense and also holds a doctorate and master's degree in Civil Law from UERJ. He is Vice President of Brasilcon Institute and Scientific Director of Iberc and a public prosecutor of the State of Rio de Janeiro.
Email: gmartins@mprj.mp.br
ORCID iD: https://orcid.org/0000-0003-3082-656X

Renata Capriolli Zocatelli Queiroz
Postdoctoral student and Doctor at the Faculty of Law of the University of São Paulo - USP. She holds a master's degree and a specialist degree from the State University of Londrina - UEL. She is a Guest Professor of the Professional Master's Program in Law, Society and Technology at the School of Law of the Londrina Colleges and a Professor of the Post-Graduate Program in Applied Business Law in the Digital Age at the State University of Londrina. She is a Professor at the Londrina Colleges. She is a lawyer.
Email: renataczqueiroz@gmail.com
ORCID iD: https://orcid.org/0000-0002-6348-751X