

LGPD: CONCEPTS, CHALLENGES AND AWARENESS IN THE NEW CULTURE FOR SOCIETY AND ORGANIZATIONS

LGPD: Conceitos, desafios e conscientização na nova cultura para a sociedade e organizações

Bárbara Palma, UFF, Brazil, <https://orcid.org/0009-0007-9644-893>

Ricardo Nolasco, UFF, Brazil, <https://orcid.org/0009-0005-7638-4025>

Daniele Sucena, UFRJ, Brazil, <https://orcid.org/0000-0003-1181-1952>

Alessandro Jatobá, Fiocruz, Brazil, <https://orcid.org/0000-0002-7059-6546>

Paulo Victor Rodrigues de Carvalho, IEN, Brazil, <https://orcid.org/0000-0002-9276-8193>

Abstract: In recent decades, there has been exponential technological growth that has directly impacted the manipulation of data in society, making information a currency of great value, especially for public and private institutions, making data governance fundamental to mitigating possible risks. of personal data leakage. In this way, the General Data Protection Law (LGPD), emerged, based on European Legislation (GDPR), to assist in the responsible processing of sensitive data and its effective implementation has become crucial for organizations to meet legal obligations and protect citizens' personal data. This work aims to demonstrate to society that organizations need to adapt to the law, presenting strategies for its implementation, in order to guarantee more assertive and secure management of sensitive data. In view of this, research was carried out through bibliographic studies on the topic, highlighting the engagement of interested parties as the main factor for success.

Keywords : LGPD, GDPR, data, security, organization and society.

Resumo: Nas últimas décadas, ocorreu um crescimento tecnológico exponencial que impactou diretamente a manipulação de dados na sociedade, tornando a informação, uma moeda de grande valor, sobretudo para as instituições públicas e privadas, tornando-se a governança de dados, fundamental para mitigar possíveis riscos de vazamento de dados pessoais. Desta forma, a Lei Geral de Proteção de

Dados (LGPD), surgiu, com base na Legislação Europeia (GDPR), para auxiliar no tratamento responsável de dados sensíveis e sua implementação eficaz se tornou crucial para que as organizações atendam as obrigações legais e protejam os dados pessoais dos cidadãos. Este trabalho tem por objetivo demonstrar à sociedade que as organizações precisam se adequarem à lei, apresentando estratégias para sua implantação, a fim de garantir uma gestão de dados sensíveis mais assertiva e segura. Diante disso, foi realizada uma pesquisa através de estudos bibliográficos sobre a temática, destacando o engajamento das partes interessadas, como o principal fator para o sucesso.

Palavras-chave: LGPD, GDPR, dados, segurança, organização e sociedade.

1. Introduction

Society has been significantly influenced by technological developments and the exponential increase in access to the internet. According to the Ministry of Health, more than 80% of the population already enjoys internet access in Brazil. This allowed us to reach a limited amount of information, making data flow control increasingly demanding (Brasil, 2023).

Along with the growing value of data and its inappropriate and abusive use, undesirable consequences for people have arisen. And whether in the physical or digital environment, data has been used, shared, sold or leaked without the consent of citizens, as well as without the ethical awareness of institutions (Mulgan; Straub, 2019).

This information traffic ends up causing vulnerabilities that, in the absence of effective management, can give rise to security breaches. This is especially concerning in government and business environments, where inappropriate exposure of sensitive information can result in data leaks or attacks by hackers who see this scenario as an opportunity. Therefore, there is a pressing need to adopt predictive strategies to combat third-party data theft, as well as investing in specialized labor that can guide and implement security measures (Rapostoo et al., 2019).

The General Personal Data Protection Law (LGPD) emerged to meet the need to establish standardization for the protection of information and it affects not only individuals, but directly institutions that will need to immediately adapt to comply with the requirements of the new law, otherwise they will suffer legal penalties for the misuse of third party data. A new business culture emerges and new habits will be necessary to overcome the challenges of maintaining compliance and effective data management (Silva; Jales, 2022).

This work describes the LGPD, what it covers, the challenges that society and organizations may encounter, subsidies to adapt it, creating engagement between interested parties and a new culture, especially related to the awareness of parties involved in the data processing process personal.

2. The LGPD

The General Data Protection Regulation (or General Data Protection Regulation - GDPR) established in 2018, in the European Union, contributed to boosting the drafting of the General Data Protection Law (LGPD) or Law 13,709, in Brazil (Almeida; Soares, 2022).

Brazil's initiative to regulate the use of data came from the need to monitor the competitiveness of the European market, where it contributed to the LGPD having significant similarities with the GDPR and also being an important aspect for attracting and retaining businesses and customers from other countries. (Pohlmann, 2019).

In Brazil, it was already possible to observe this concern through the existence of sectoral standards on the subject and mechanisms applicable to data protection contained in the Access to Information Law, Positive Registration Law, Marco Civil da Internet, Federal Constitution, Code of Defense of Consumer and Civil Code (Almeida; Soares, 2022).

Adopted in August 2018, the LGPD aims to improve the governance of citizens' personal data within institutions, addressing the processing and protection of data from legal entities and individuals, in addition, designating responsibility for the management of personal data in the country, the National Data Protection Authority (ANPD) (Silva; Jales, 2022). In this way, it aims to guarantee freedom and essential privacy rights protected.

3. Fundamentals

The law mentions in its article 2 the following grounds regarding the protection of personal data (Brasil, 2018, p. 01):

I - respect for privacy;

II - informative self-determination;

III - freedom of expression, information, communication and opinion;

IV - the inviolability of intimacy, honor and image;

V - economic and technological development and innovation;

VI - free enterprise, free competition and consumer protection; It is

VII - human rights, the free development of personality, dignity and the exercise of citizenship by natural persons.

According to Oliveira (2021), the LGPD establishes a series of principles that should guide the processing of personal data. Here are the 10 basic principles:

1. Purpose: Data processing must have legitimate, specific, explicit and informed purposes.

2. Suitability: The processing must be compatible with the established purposes.
3. Necessity: Only the data strictly necessary to achieve the proposed purposes must be used.
4. Free Access: Holders have the right to access their data and obtain complete information about them.
5. Data Quality: Data must be accurate, clear, relevant and updated.
6. Transparency: Information on data processing must be made available in a clear, precise and easily accessible way to data subjects.
7. Security: Technical and administrative measures must be adopted to protect personal data.
8. Prevention: Measures must be taken to avoid harm to data subjects.
9. Responsibility and Accountability: Those responsible for processing data must demonstrate that they have adopted effective measures to comply with personal data protection standards.
10. Non-Discrimination: Personal data must not be used for discriminatory, illegal or abusive purposes.

4. Main Actors Involved

The LGPD clearly establishes who is considered the holder of personal data and who are the people involved in the processing of this data, the controller, the operator, the person in charge and the national authority (Brasil, 2018).

a) Holder

The data subject is the natural person to whom the personal data that is subject to processing refers. It is fundamental in the context of data processing, since it is the person affected by any security incidents that may occur with your personal data (Brazil, 2018).

The holder is the individual holding the data that is subject to processing. Even when we fill out a registration form and provide our personal data for the company to store, we continue to be the holders of that data (Brazil, 2018).

The LGPD establishes the rights of the data subject. Furthermore, the same article establishes that these rights can be exercised at any time with the controller, upon request (Brazil, 2018).

b) Controller

The controller, which is the entity, whether an individual or a legal entity governed by public or private law, that makes decisions regarding the processing of personal data, does not necessarily need to be a natural person; this implies

that companies, committees and working groups can also perform this function (Donda, 2021).

In general terms, the role of controller is performed by a legal entity, whether under private or public law. According to the ANPD, natural persons who act as professionals subordinate to a legal entity or as members of its bodies are not considered controllers. This prevents the specific responsibilities of a legal entity from being assigned to a natural person acting on behalf of the legal entity. On the other hand, a natural person who acts independently, such as individual entrepreneurs and independent professionals, can be considered controller and, therefore, responsible for the processing of personal data in their activities. Among the decisions to be made by the controller is the purpose of the processing, the nature of the personal data processed and the duration of the processing (Brasil, 2021).

c) Operator

Similar to the controller, the operator is defined as the natural or legal person, governed by private or public law, who processes personal data on behalf of the controller. Likewise, the processing must be carried out in accordance with the instructions provided by the controller, who will supervise compliance with its own instructions and the rules related to the matter (Brazil, 2018).

The operator is the entity that processes personal data on behalf of the controller. Both the controller and the operator have legal responsibilities related to data security and privacy. Furthermore, they are responsible for designating the DPO (Data Protection Officer), who acts as a communication link between the controller, data subjects and the National Data Protection Authority (ANPD) (Donda, 2021).

d) Person in charge

This is a person designated by the controller and operator to serve as an intermediary between the controller, data subjects and the National Data Protection Authority (ANPD) (Brazil, 2018).

The person in charge must have a professional profile suitable for data protection management, demonstrating knowledge in the areas of information security and data protection, in order to guarantee the application of best practices to the environment under their responsibility. Depending on the size of the organization, the person in charge may count on the support of a team of professionals who will assist in the task of protecting the data processed. As it is the main point of contact for receiving complaints and communications from data subjects, the person in charge must have their name and contact information publicly available (Ferreira, 2020).

The LGPD also establishes the obligation for companies that process personal data to hire a Data Protection Officer (DPO) (Ferreira, 2020). According to Cruz (2021), it is not strictly necessary to have training in information systems

to be a DPO, but it is highly recommended to have knowledge about the LGPD and be well-informed about data processing.

The activities that the Data Protection Officer (DPO) will perform, in accordance with Art. 41 § 2, according to Brasil (2018), include:

1. Take measures in response to complaints, communications from data subjects or notifications from the National Data Protection Authority (ANPD)
2. Guide employees on practices related to data protection;
3. Fulfill the duties determined by the controller;
4. National Data Protection Authority (ANPD).

The ANPD was established by the Brazilian government as the regulatory authority for monitoring and applying sanctions in cases of inappropriate data processing. It is responsible for supervising, implementing and monitoring compliance with the LGPD. Its main functions include protecting privacy, regulating compliance with the law, providing guidance, promoting awareness, monitoring and applying sanctions (Maciel, 2019).

When it comes to personal data security incidents, the ANPD acts as an administrative body, intervening after direct resolution options with the controller and the organization responsible for the data have been exhausted. The ANPD conducts its administrative processes, guaranteeing the right to adversarial proceedings, full defense and appeal. Furthermore, its performance is guided by minimal intervention, while ensuring respect for the foundations, principles and rights of holders, as established in the LGPD and the Federal Constitution (Brazil, 2018).

Furthermore, it must collaborate and coordinate its actions with other bodies and entities that have normative and sanctioning powers, becoming the central body responsible for interpreting the LGPD and establishing standards for its implementation. Only the ANPD is authorized to impose the sanctions provided for in the LGPD (Brazil, 2018).

5. Lgpd Adjustment Process

For Cunha et al. (2021), the complexity of the changes introduced by the LGPD, especially in countries without a consolidated data protection culture, understanding how to adapt can be challenging. Therefore, the most recommended approach to the adaptation process is to involve the entire organization and society, forming multidisciplinary working groups in the business areas responsible for processing personal data, as well as coordinating information security and transparency with the public.

According to the author, external professionals and clients can also be incorporated into this process, contributing to unified strategies and procedures. Each company has the flexibility to create a structure that best adapts to its reality, opportunities and financial capacity. This collaborative and comprehensive approach is useful for effective and sustainable implementation of the LGPD.

The main potential advantages are reduced expenses, risk prevention, behavioral guidelines designed to raise employee awareness and the identification and anticipation of possible adverse situations (Severino, 2020).

According to Lima (2021), companies will also be able to develop our preferences and consumption profiles, based on the information collected, even making predictions about our future behavior. In addition to benefiting the private sector, this data also generates significant social and economic advances for the public sector. They allow people to recognize, filter and extract value from data relating to public policies, facilitating more informed decision-making. Additionally, they provide new real-time insights and predictions on how to act to face challenges and discover new opportunities.

The main challenges of the LGPD were that it was enacted in 2018, but it only became effective in 2020. This postponement, which was considerably prolonged, proved to be indispensable to allow companies to adapt to the new requirements. This involves aspects related to data storage, costs, specialized advice and employee training (Melo Filho; Pereira; Queiroga, 2023)

However, when the LGPD came into force, few organizations were properly prepared. In fact, most of them were skeptical about the effective implementation of the law, even after it came into effect. Furthermore, some companies did not consider compliance with the LGPD as a priority in their plans, even in the face of alarming news about the harmful impact of neglecting personal data on people's privacy and freedom (Teixeira et al., 2021).

In 2019, the company Serasa Experian conducted a survey with the aim of evaluating the perception of consumers and companies in relation to the LGPD. The study involved 1,564 participants and revealed that 85% of them did not have knowledge on the subject of data processing required by law. With regard to 508 companies, with 18 sectors of activity, were surveyed and 66% reported having an intermediate understanding of the law. Understanding the principles and our rights in relation to the processing of personal data is extremely important, as is knowledge of the legal responsibilities associated with this topic and 72% of small businesses intend to hire specialized professionals (Serasa Experian, 2019).

According to Teixeira et al. (2021), this behavior of national companies and public bodies is not surprising, as it reflects the culture of Brazilian business, characterized by the attitude of "waiting to see what happens" or the belief that they will never face concrete risk situations. In this context, some pertinent questions arise. According to the author, although technical and administrative measures can contribute to compliance with the law, they will only generate effective results if they encounter little resistance from employees. It is crucial

to recognize that, in the triad of "processes, technology and people", the human element can be the determining factor in the success or failure of actions.

It is also observed that it is common for all new legislation, as well as the LGPD, to present two main difficulties: interpretation, which still needs to be firmly established, and implementation, which is not a simple task. With regard to the first question, the challenge lies in establishing solid interpretative structures for the LGPD, in a segmented manner, from which judicial interpretation and the actions of supervisory authorities, in particular the ANPD, can be derived. As for the second aspect, the challenge is to ensure that compliance with legal obligations does not harm the viability of organizational processes (Teixeira et al., 2021).

And with this, companies have realized the importance of being in compliance with the LGPD and established an indispensable requirement, especially to promote solid internal relationships, build successful external partnerships and define the image and values that the company will transmit to the public (Rocha, 2021). And one of the steps to achieve this objective, according to Teixeira et al. (2021), is to involve the entire team by creating awareness through educational initiatives.

Leaders must be educated that compliance with the LGPD is not limited to a single action, such as purchasing a system or incorporating/changing a procedure. It is, in fact, a set of actions that covers strategy, governance, policies, procedures, tools, change management, awareness, training, monitoring, responsibility, transparency, among other elements (Aguiar, 2021).

6. The Culture of Data Privacy

The LGPD brought with it the need to raise awareness throughout society regarding the importance of personal data and its impacts on the individual's essential rights and guarantees, especially with regard to freedom, privacy and free personal development (Mulgan; Straub, 2019).

For Zavarella et al. (2023), one of the main challenges in the process of adapting to the LGPD in the company consists of incorporating a new organizational culture, focusing on data protection, involving the participation and engagement of all employees and society, as well as reflecting the importance of confidentiality of personal and/or sensitive data of candidates and employees, aiming to protect both parties (holder and company) against undue exposure or fraud.

Establishing a culture of privacy involves considering two dimensions: the rational (intellectual) dimension and the axiological dimension (values). In addition to understanding the technical aspects of the LGPD, it is equally crucial to internalize its value within the organization. Each of them, in a unique way, guidance and awareness, play an important role in building a culture of privacy and data protection within an organization (Lima, 2021).

In practice, the rational dimension is achieved through guidance, which involves teaching the technical aspects of what should be done. On the other hand, the axiological dimension is achieved through awareness, which consists of educating people about the importance of respecting the rights of data subjects (Teixeira et al., 2021).

Training must be specifically targeted and relevant to everyday activities, allowing understanding of the cybersecurity implications arising from their actions, as well as the regulations related to the protection of personal data (Stelzer et al., 2019).

The LGPD establishes as a primary requirement the training of professionals responsible for processing personal data. In this context, several organizations and companies provide specialized training and courses in data protection and compliance with the LGPD. These educational programs equip employees and can extend to citizens with the necessary knowledge to implement appropriate data protection measures, thus promoting a safe environment that complies with the law (Tepedino; Frazão; Oliva, 2020).

In relation to training, the law defines the controller's commitment to adopting internal processes and policies, ensuring compliance with standards and good practices related to the protection of personal data, which is essential for the success of the Privacy Governance Program (PGP). This commitment can be strengthened through the implementation of training and development programs (Brazil, 2018).

According to Jacoby and Camarão (2020), the implementation of a new policy or action generally requires training to instruct and strengthen best practices, in addition to verifying learning and retention of information. This represents a behavioral change, requiring commitment from users and, consequently, requires attention, time and monitoring to consolidate this new stance, which is not a preference, but a legal duty.

According to Bonjour (2023), training is essential to ensure that all teams are in tune with LGPD requirements and are able to deal with personal information. Additionally, training is a way to raise awareness among employees about the importance of preserving personal data and the privacy of the holders of this information.

Regarding methodology, there are several approaches to training employees on the LGPD. It is crucial to select an efficient method that is aligned with the company's specific needs. Among the available options, in-person training, online courses and workshops stand out. Regardless of the chosen modality, it is imperative that the training is comprehensive, covering everything from basic concepts to the necessary security measures according to the LGPD (Bonjour, 2023).

The level of qualified training and knowledge acquired will vary according to the positions and responsibilities performed. This training covers several topics,

including the introduction to Brazilian data protection law, the main concepts of the LGPD, consent related to data processing and the rights of the holder, in addition to the processing of sensitive personal data, which have the purpose of improving the relationship with the customer, making proposals more transparent and clear. Although this training is theoretical and can be tiring due to the details of the topics, a more didactic approach can be useful to transmit this knowledge (Cunha et al., 2021).

According to Jacoby and Camarão (2020), it is recommended to develop a training plan that ensures cohesion throughout the various learning stages, adapting to the specific needs of each public body or entity.

The purpose of the training is to ensure that all employees are aligned with legal requirements, understanding how to handle personal data securely and in accordance with regulations (Bonjour, 2023). For Cunha et al. (2021), serves to improve performance and quality of service. If teams follow the rules correctly, benefits will be easily achieved and company data will be secure.

7. Conclusion

The implementation of the LGPD is not without challenges. One of the main obstacles faced by organizations is ensuring compliance with legal requirements. This requires a comprehensive review of internal policies, the adoption of robust security measures, and the implementation of effective data governance practices. Furthermore, organizational culture plays a crucial role in adapting to the LGPD. Changing mindsets and raising awareness about the importance of data protection at all levels of the company are essential to ensuring continuous and effective compliance.

Furthermore, awareness about LGPD is not just limited to organizations, but also extends to society in general. Citizens need to understand their rights in relation to their personal data and be aware of the measures they can take to protect their privacy. This includes understanding how your information is being collected, used and protected by organizations, as well as exercising your rights to access, rectify and delete data.

In summary, the LGPD represents a significant advance in protecting the privacy and rights of individuals in relation to their personal data. However, its effectiveness depends not only on the compliance of organizations, but also on the awareness and engagement of society as a whole. Only through a comprehensive and collaborative approach will it be possible to promote a new culture of data protection that benefits both organizations and citizens.

When implemented in information technology companies, the General Data Protection Law establishes a standard not only for the organization's security, but also for the protection of the data of customers and users who are involved with the company's services and products. The LGPD introduces an approach

that seeks to adapt corporate habits to business reality, in which data, even though it is the most valuable resource, must be treated with extreme sensitivity.

The objective of this work was to simplify the understanding of the principles and foundations of the General Personal Data Protection Law, as well as its application, especially in the business context, in its processes that raise awareness and benefit society.

Among the crucial actions that a company must implement, the importance of ensuring the holder's consent regarding the data that will be used can be highlighted. In other words, the data subject must have full access to their data at any time, understand the purpose of its use and agree to that purpose. In addition to consent, there are other fundamental measures to be adopted to ensure compliance with the standards established by the LGPD.

Acquiring training in compliance with the LGPD is necessary to ensure the protection of personal data and prevent legal violations. All areas of the company that deal with personal information must be included in this training, which can be taught in person, online or through workshops. In addition to mitigating the risks associated with LGPD violations, training plays a fundamental role in raising employees' awareness of the importance of preserving personal data and the privacy of information holders. This effort helps to strengthen the company's image among customers and society in general.

Investing in LGPD training is a crucial measure to ensure the security of personal data and prevent potential complications. In addition to training, communication and comprehensive dissemination of the subject contribute to fostering a cultural change in the organizational environment, highlighting the responsibility in handling personal data and seeking to raise awareness of all individuals and customers involved.

It was presented that the implementation of security measures and the adoption of good practices in managing employee data are essential. These actions aim to protect employees against vulnerable situations that could result in labor disputes before judicial authorities and regulatory bodies. It is essential that all efforts represent an authentic paradigm shift, adapting corporate culture to the new reality defined by the information age, also known as generation 4.0. This transformation requires the effective change of habits and customs of everyone involved in the process. The implementation of effective governance of employee data is necessary to avoid moral and financial losses for the company.

References

Aguiar, Tiago Lopes de. Guia de Conformidade: Lei Geral de Proteção de Dados Pessoais (LGPD). SETIC - Secretaria de Tecnologia da Informação e Comunicação. Governo do Estado de Rondônia. Porto Velho/ RO, 2021. Disponível em: <https://rondonia.ro.gov.br/wp-content/uploads/2022/09/Guia->

de-Conformidade-LGPD-SETIC-versao-1.0.pdf.

Almeida, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. *Perspectivas em Ciência da Informação*, v.27, n. 3, p. 26-45, jul/set 2022.

Alves, Gervânia. Ciclo de Vida dos Dados e LGPD. Site Xpositum. 2020. Disponível em: <https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd>.

Associação Brasileira de Normas Técnicas. ABNT NBR 10520: informação e documentação: citações em documentos: apresentação. Rio de Janeiro: ABNT, 2002.

Associação Brasileira de Normas Técnicas. ABNT NBR 27000: Princípios e Vocabulário, define a nomenclatura utilizada nas normas seguintes da família 27000. ABNT, 2014.

Atheniense, Alexandre. LGPD Para Empresas. Belo Horizonte: 2019. E-book. Página 28. Disponível em: https://www.alexandreatheniense.com.br/wpcontent/uploads/2019/07/ebook_guia_

Azevedo, Reinaldo. Nova falha do Ministério da Saúde expõe dados de 200 milhões de brasileiros. Site Uol, 2020. Disponível em: <https://noticias.uol.com.br/colunas/reinaldo-azevedo/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-200-milhoes-de-brasileiros.htm>.

Bélanger, France; Crossler, Robert E. Privacy in the digital age: a review of information privacy research in information systems. *Mis Quarterly*, v. 35, n. 4, p. 1017-1041, dez. 2011.

Brasil. ANPD - Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Versão 2. Abril, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado_defeso_eleitoral.pdf

Brasil. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

Brasil. Guia de Elaboração de Programa de Governança em Privacidade. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf>.

Brasil. Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei 13.709 de 14 de Agosto de 2018. Segurança em Banco de Dados para Adequação a LGPD, 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

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

Brasil. Ministério das Comunicações. Conectividade: 80% dos domicílios brasileiros possuem acesso à internet, aponta pesquisa. Brasília, 2023. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2023/maio/80-dos-domicilios-brasileiros-possuem-acesso-a-internet-aponta-pesquisa>.

Bonjour, Victor. Treinamento LGPD: como garantir a conformidade e evitar sanções treinando a equipe. Site Twygo, 2023.

Brandão Graziela. Mapeamento de Dados: O que é e como fazer data mapping. BL Consultoria Digital, 27 Feb. 2020. Disponível em: <https://blconsultoriadigital.com.br/mapeamento-de-dados/>.

Castilho, Luiz Ricardo de. O que podemos aprender com ano marcado por casos de vazamentos de dados. Site Consultor Jurídico, 2022. Disponível em: <https://www.conjur.com.br/2022-abr-19/luiz-castilho-casos-vazamentos-dados2/>.

Cervo, Amado Luiz. Metodologia científica: para uso dos estudantes universitários. Amado Luiz Certo e Pedro Alcino Bervian. 3.ed. São Paulo, McGraw-Hill do Brasil, 1983.

Cruz, Danielle da Costa Santos. A Lei Geral de Proteção de Dados Pessoais (LGPD): contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. Disponível em: bdta.ufra.edu.br/jspui/handle/123456789/1711.

Cunha, Blenda Eduarda de Melo.; PEREIRA, Esdras Dalmo Pinto; TIM-OTEO, Geovana; BARBOSA, João Victor Arruda; ASSIS, Maria Eduarda de; ALMEIDA, Maria Eduarda Moreira. As dificuldades de implementação da LGPD no Brasil. Revista Projetos Extensionistas, v.1, n. 2, p. 39-47, jul./dez. Faculdade de Pará de Minas/MG - FAPAM, 2021. Disponível em: <https://periodicos.fapam.edu.br/index.php/RPE/article/view/391/249>.

Donda, D. Guia Prático de Implementação da LGPD. Segurança em Banco de Dados para Adequação a LGPD. São Paulo: Labrador, 2020.

Duarte, Raiana Caberlon; NEUMANN, Andressa Maria Dias. A busca incessante pela proteção de dados pessoais na sociedade atual sob a ótica da lei 13. 709/18. Anuário pesquisa e extensão UNOESC São Miguel do Oeste – 2021.

Ferreira , F. LGPD: por que você não pode mais esperar para se adaptar, 2020. Disponível em: <https://lozinskyconsultoria.com.br/estrategia-e-gestao-de-ti/lgpd-por-que-voce-nao-pode-mais-esperar-para-se-adaptar/>.

Freitas, Alfredo. Compliance: O Guia Essencial. Portal Direito Profissional. jun. 2019. Disponível em: <https://www.direitoprofissional.com/compliance/>.

Jacoby, Murilo; Camarão , Tatiana. Ponderações sobre a Lei Geral de Proteção de Dados Pessoais no poder público. LGPD e Administração Pública - Ed. 2020. Disponível em: <https://direitodofuturo.uff.br/wp-content/uploads/sites/324/2022/05/ARTIGO-7.pdf>.

Kalloniatis, C.; Kavakli, E.; Gritzalis, S.: Addressing privacy requirements in system design: the PriS method. *Requirements Engineering*. v.13, pp. 241-255, 2008.

Karyda, Maria; MITROU, Lilian. *Data Breach Notification: Issues and Challenges for Security Management (2016)*. MCIS 2016 Proceedings. 60. Disponível em: <https://aisel.aisnet.org/mcis2016/60/>.

Kiyohara, Jefferson. *A importância do PMO na adequação a LGPD*. 2019. Disponível em: <https://lexprime.com.br/2019/09/a-importancia-do-pmo-na-adequacao-a-lgpd>.

Konder, Carlos. Privacidade e corpo: convergências possíveis. *Pensar, Fortaleza*, v. 18, n. 2, maio-ago. 2013, p. 354-400. Disponível em: <https://periodicos.unifor.br/rpen/article/view/2696/pdf>.

Lima, Daniela Cenci. *Lei Geral de Proteção de Dados: Um Guia Breve e Simples*. Defensoria Pública do Estado do Rio Grande do Sul, Abril, 2021.

Lohmann , Pedro A.; Albuquerque, Carlos; Machado, Raphael. *Revisão Sistemática para o Processo de Avaliação de Impacto sobre a Proteção de Dados Pessoais e à Privacidade*. Niterói, 2020. Disponível em https://www.researchgate.net/publication/349924412_Revisao_Sistematica_para_o_Processo_de_Avaliacao.

Maciel, Rafael Fernandes. *Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei no 13.709/18)*. RM Digital Education. 1a Edição. Goiânia – GO. 2019.

Máximo, Welton. BC comunica vazamento de dados de 2,1 mil chaves Pix: Foram vazados dados cadastrais da Logbank Pagamentos. *Economia: Agência Brasil - Brasília*, 2022. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2022-02/bc-comunica-vazamento-de-dados-de-21-mil-chaves-pix>.

Melo Filho, Djunio Rosa de; PEREIRA, José Vitor de Aguiar; QUEIROGA, Thiago Abreu Campelo. *Metodologia Scrum: Uma aliada na implementação da LGPD*. *Research, Society and Development*, v. 12, n. 4, e22712441189, 2023. Disponível em: <https://rsdjournal.org/index.php/rsd/article/view/41189/33553>.

Mulgan, Geoff; STRAUB, Vicent. *The new ecosystem of trust*. Blog: Site Nesta, 2019. Disponível em: <https://www.nesta.org.uk/blog/new-ecosystem-trust/>.

Neri, Leonardo. *LGPD – as fases de implementação de um programa de privacidade*. Site Mazzuco e Mello, 2020. Disponível em: <https://www.mazzuccoemello.com/lgpd-as-fases-de-implementacao-de-um-programa-de-privacidade/>.

Okano, Marcelo T.; Ferreira, Lamara; Lobo dos Santos, Henry de Castro; URSINI, Edson L. *LGPD: O Novo Desafio para as Organizações - Exemplos de Frameworks para Diagnosticar Este Novo Cenário*. *South American Development Society Journal*, Vol. 07, No. 20, 2021.

Oliveira, Germano Frota Sá de. LGPD: um estudo sobre os desafios e benefícios da implantação em empresas. Dissertação para o Curso de sistema da Informação - Unifametro. Fortaleza, 2021.

Pierson, C. T. Data Breaches Highlight the Importance of Privacy. *Financial Executive*, Morristown, NJ, v. 25, n. 2, p. 62-63, 2009.

Pinheiro, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD). Editora Saraiva, 2021, p25. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>.

Pohlmann, Sérgio. LGPD Ninja: Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas. 1. ed. Novo Friburgo: Editora Fross, 2019. 240 p., v. 1. Disponível em: <https://dokumen.pub/lgpd-ninja-entendendo-e-implementando-a-lei-geral-de-proteao-de-dados-na-empresa-1nbsped-9781089345886-1089345887.html>

Rajasekharan, D. Accelerate Your Response to the EU General Data Protection Regulation (GDPR). Oracle White Paper, 2017. Disponível em: <https://www.oracle.com/technetwork/database/security/wp-security-dbsec-gdpr3073228.pdf>.

Rapôso, Cláudio Felipe Lima et al. LGPD-lei geral de proteção de dados pessoais em tecnologia da informação: revisão sistemática. *RACE Revista da Administração*. V. 4, p. 58-67, 2019.

Reuters, Thomson. O que meu escritório contábil precisa saber sobre LGPD?, 2020. Disponível em: <https://www.dominiosistemas.com.br/blog/o-que-meu-escritorio-contabil>.

Rocha, Cláudio Jannotti da; PONTINI, Milena Souza. Compliance trabalhista: impacto da lei geral de proteção de dados (lgpd) no direito do trabalho. Lisboa: *Revista Jurídica Luso Brasileira*. 04 fev. 2021.

Rodotà, Stefano. A vida na sociedade da vigilância. A privacidade hoje. Rio de Janeiro: Renovar, 2008. Tradução: Danilo Doneda e Luciana Cabral Doneda.

Sambrana, Carlos. Novo vazamento expõe mais de 100 milhões de contas de celular. *Insiders: Neofeed*, 2021. Disponível em: <https://neofeed.com.br/blog/home/exclusivo-novo-vazamento-expoe-mais-de-100-milhoes-de-contas-de-celular/>.

Santos, André Ricardo Matos dos; REIS, Carlos Henrique Sucupira; FERNANDES, Maria Eduarda Alves Siqueira. A aplicação da Lei Geral de Proteção de Dados em privacidade e segurança, a partir da sua inicialização nas empresas de tecnologia da informação no Distrito Federal. Núcleo Interdisciplinar de Pesquisa. *Centro Universitário de Desenvolvimento do Centro-Oeste*. v. 1, n. 1, 2022.

Santos, Fernanda Cristina Soares. O consentimento no contexto da proteção de dados pessoais. Site Lage e Portilho Jardim. Belo Horizonte, 2021. Disponível em: <https://lageportilhojardim.com.br/blog/consentimento-lgpd/>.

Santos, Flávia Alcassa dos. A Lei Geral de Proteção de Dados Pessoais (LGPD) e a Exposição de Dados Sensíveis nas Relações de Trabalho. Revista do Tribunal Regional do Trabalho da 10ª Região, Brasília, v. 24, n. 2, 2020.

Serasa Experian. 85% das empresas declaram que ainda não estão prontas para atender às exigências da Lei de Proteção de Dados Pessoais, mostra pesquisa da Serasa Experian. Estudos e Pesquisas. 2019. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/estudos-e-pesquisas/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender-as-exigencias-da-lei-de-protecao-de-dados-pessoais-mostra-pesquisa-da-serasa-experian/>.

Severino, Dandara Benedett. O compliance trabalhista e sua aplicação na esfera empresarial. Monografia. Universidade do Sul de Santa Catarina. Tubarão, 2019.

Silva, Indira D. O. T.; JALES, José L. de A. O impacto da nova LGPD (Lei Geral de Proteção de Dados. Trabalho para conclusão de curso. Universidade Potiguar. Natal, 2022.

Silveira, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. Privacy and the Market of personal data. Liinc em Revista, v. 12, n. 2, 2016.

Soares, Nycolle Araújo; MARTINS, Rafael Lara. LGPD: Lei Geral de Proteção de Dados. 2020. Disponível em: <https://www.laramartinsadvoga-dos.com.br/wp-content/uploads/2020/08/Ebook-1-1.pdf>.

Stelzer, Joana. Gonçalves, Everton Das Neves; Baptista, Rudá Ryuiti Furukita; VAZ, Rafael Medeiros Popini; WIEIRA, Keite; FIDELIS, Monique De Medeiros. A Lei Geral de Proteção de Dados Pessoais e os desafios das Instituições de Ensino Superior para a adequação. XIX Colóquio Internacional de Gestão Universitária. Santa Catarina, Rio Grande do Sul, 2019.

TCU - Tribunal De Contas Da União. Boas práticas em segurança da informação. 2. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007.

Teixeira et al. LGPD E Cartórios implementação e questões práticas. São Paulo: Saraiva Jur, 2021.

Tepedino, Gustavo.; Oliva, Milena Donato; Frazão, Ana. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais. São Paulo/SP, 2020. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/138898/SUMARIO_lei_geral_protecao_tepedino_2020.pdf.

Totvs. Como implementar o compliance trabalhista na empresa?. Adequação à legislação. Totvs, 2020. Disponível em: <https://www.totvs.com/blog/adequacao-a-legislacao/compliance-trabalhista/>.

Vasconcellos Junior, Carlos Augusto Pinto; Ferreira, Victor Silva. Impacto

da Lei Geral de Proteção de Dados Pessoais nas relações de Trabalho: a necessidade de implantação do programa de integridade (compliance). Laboratório UERJ de Trabalho e Previdência (LABUTA), 2020. Disponível em: <https://uerjla-buta.com/2020/03/21/impacto-da-lei-geral-de-protecao-de-dados-pessoais-nas-rela-coes-de-trabalho-a-necessidade-de-implantacao-do-programa-de-integridade-com-pliance/>.

Willemsen, B. The World's Most Important Gathering of CIOs and IT Executives. Gartner IT Symposium/Xpo. Orlando/FL, 2019. Disponível em: <http://www.gartner.com/br/symposium>.

Zavanella , Fabiano et. al. Direito do trabalho e gestão corporativa. LTr Editora, São Paulo, 2023.