Cognitio Juris
ISSN 2236-3009

UM OLHAR SOBRE A SEGURANÇA DE DADOS PESSOAIS

A LOOK AT PERSONAL DATA SECURITY

Artigo submetido em 27 de novembro de 2023
Artigo aprovado em 02 de dezembro de 2023
Artigo publicado em 05 de dezembro de 2023

Cognitio Juris
Volume 13 – Número 52 – Dezembro de 2023
ISSN 2236-3009

.

Autor(es):
Victor Coelho Bignardi Garcia Silveira [1]

.

RESUMO: Este trabalho tem como tema a segurança de dados pessoais, amparado por aspectos legais com a Lei Geral de Proteção de Dados (LGPD), que regula o uso de dados pessoais. A LGPD e necessária para garantir os direitos e deveres dos titulares e dos agentes de tratamento de dados. A hipótese é que a LGPD é um avanço na legislação brasileira, mas que precisa de mais ações para sua efetivação e fiscalização. A segurança de dados pessoais e fundamentais para garantir a proteção e a privacidade dos indivíduos e das organizações na era digital. Ela vem por meio de um conjunto de medidas técnicas, administrativas e jurídicas que visam preservar a confidencialidade, a integridade e a disponibilidade das informações, independentemente do seu formato ou meio de armazenamento. Ela se

relaciona com o tratamento adequado dos dados que identificam ou tornam identificável uma pessoa natural, respeitando os seus direitos fundamentais e as normas legais aplicáveis. Desse modo, tem-se uma abordagem multidisciplinar e uma constante atualização dos conhecimentos e das práticas, tendo em vista os desafios e as ameaças que surgem no cenário cibernético. Além disso, é existe a necessidade de conscientizar os usuários e os responsáveis pelas informações e pelos dados pessoais sobre a importância de adotar boas práticas de segurança. Essa pesquisa utiliza de meios bibliográficos para analisar e evidenciar a importância, as oportunidades e os desafios relacionados a segurança de dados.

Palavras-chave: LGPD, segurança de dados, importância e desafios.

Abstract: This work has as its theme the security of personal data, supported by legal aspects with the General Data Protection Law (LGPD), which regulates the use of personal data. The LGPD is necessary to guarantee the rights and duties of data subjects and data processing agents. The hypothesis is that the LGPD is an advance in Brazilian legislation, but it needs more actions for its effectiveness and monitoring. The security of personal data is fundamental to guarantee the protection and privacy of individuals and organizations in the digital age. It comes through a set of technical, administrative and legal measures that aim to preserve the confidentiality, integrity and availability of information, regardless of its format or storage medium. It relates to the proper treatment of data that identifies or makes a natural person identifiable, respecting their fundamental rights and applicable legal norms. Thus, a multidisciplinary approach and constant updating of knowledge and practices are required, considering the challenges and threats that arise in the cyber scenario. In addition, there is a need to raise awareness among users and those responsible for information and personal data about the importance of adopting good security practices. This research uses bibliographic means to analyze and highlight the importance, opportunities and challenges related to data security.

Keywords: LGPD, data security, importance and challenges.

INTRODUÇÃO

A segurança de dados pessoais é um tema cada vez mais relevante na sociedade contemporânea, especialmente diante do avanço das tecnologias digitais e da crescente exposição das informações pessoais na internet. Nesse contexto, surge a Lei Geral de Proteção de Dados (LGPD), que visa regulamentar o tratamento de dados pessoais pelos agentes públicos e privados, garantindo os direitos fundamentais de liberdade, intimidade e privacidade dos titulares dos dados.

O objetivo deste trabalho é analisar a importância da LGPD para a proteção dos dados pessoais, bem como os desafios e as oportunidades que ela traz para os diversos setores da sociedade. Para isso, será realizada uma pesquisa bibliográfica, baseada em livros e artigos sobre o tema. A hipótese central é que a LGPD representa um avanço significativo na legislação brasileira sobre a matéria, mas que ainda há muito a ser feito para que ela seja efetivamente implementada e fiscalizada, garantindo assim os direitos e deveres dos envolvidos no tratamento de dados pessoais.

CAPÍTULO 1

1. **A segurança digital e sua interação com a lei**

Nesse primeiro capítulo será abordado o tema segurança de informação digital e sua interação com a lei, especialmente no contexto brasileiro. A segurança de informação digital é o conjunto de medidas que visam proteger os dados pessoais e corporativos, que circulam no ambiente virtual contra ameaças como ataques cibernéticos, vazamentos, fraudes, entre outras. A lei é um instrumento que regula e normatiza as relações jurídicas que envolvem o tratamento de dados digitais, estabelecendo direitos e deveres para os agentes envolvidos, como titulares, controladores, operadores e autoridades competentes.

Neste capítulo, serão apresentados os principais conceitos e princípios relacionados à

segurança de informação digital e à lei, bem como as normas vigentes no Brasil sobre o assunto, com destaque para a Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em 2020. Além disso, serão discutidos os desafios e as tendências para o aprimoramento da segurança de informação digital e da legislação correlata, diante do cenário em constante evolução tecnológica e social. Conforme consta no Artigo 1º:

[...] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. [...]. (GUERREIRO, 2022, p.38) 1

A segurança da informação digital é um conjunto de medidas que visa proteger os dados e as informações de ameaças internas e externas, garantindo a sua confidencialidade, integridade, disponibilidade e autenticidade. Esses são os quatro princípios básicos da segurança da informação, que devem ser seguidos por todas as empresas e organizações que lidam com dados sensíveis ou estratégicos.

A confidencialidade se refere à privacidade dos dados, ou seja, ao acesso restrito às informações apenas às pessoas autorizadas. A integridade se refere à veracidade dos dados, ou seja, à garantia de que os dados não sejam alterados ou corrompidos sem autorização. A disponibilidade se refere à acessibilidade dos dados, ou seja, à garantia de que os dados estejam disponíveis quando necessários. A autenticidade se refere à origem dos dados, ou seja, à garantia de que os dados sejam autênticos e que a identidade do remetente seja verificada.

Além desses quatro princípios, há também o princípio da legalidade, que se refere ao

cumprimento das leis e normas vigentes sobre a proteção dos dados e das informações. No Brasil, a principal lei que regula a segurança da informação digital é a Lei Geral de Proteção de Dados (LGPD), passou a multar as empresas em 2021 por violações aos direitos dos titulares dos dados.

A segurança da informação digital é essencial para evitar prejuízos financeiros, reputacionais e legais para as empresas e organizações, bem como para proteger os direitos e interesses dos titulares dos dados. Por isso, é importante que as empresas adotem boas práticas de segurança da informação digital.

[...] a compreensão do âmbito de proteção de um direito fundamental à proteção de dados pessoais envolve sempre um contraste com o de outros direitos, destacando-se, nesse contexto, o direito à privacidade e o direito à autodeterminação informativa, os quais, por seu turno, embora também autônomos entre si, também apresentam zonas de contato importantes [...]. (DONEDA, 2022, p.95) 2

A citação expressa uma visão sobre o direito fundamental à proteção de dados pessoais, que é reconhecido pela Constituição Federal e pela Lei Geral de Proteção de Dados Pessoais. Esse direito visa garantir que os cidadãos tenham controle sobre suas informações pessoais, que são coletadas e tratadas por diversos agentes na sociedade da informação. No entanto, esse direito não é absoluto, e deve ser ponderado com outros direitos fundamentais, como o direito à privacidade e o direito à autodeterminação informativa.

O direito à privacidade se refere à proteção da intimidade, da honra e da imagem das pessoas, impedindo que seus dados sejam expostos ou violados sem o seu consentimento. O direito à autodeterminação informativa se refere à capacidade das pessoas de decidirem sobre o uso e a divulgação de seus dados, podendo acessá-los, corrigi-los ou excluí-los. Esses dois direitos estão relacionados ao direito à proteção de dados pessoais, mas também possuem especificidades e autonomia. Por isso, é necessário compreender o âmbito de cada

um deles, e buscar um equilíbrio entre eles, respeitando os princípios e as normas que regem a matéria.

LGPD tem como objetivo garantir os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade das pessoas naturais, regulando o tratamento de dados pessoais por pessoas físicas ou jurídicas, públicas ou privadas, nos meios físicos ou digitais.

A LGPD aplica-se a qualquer tratamento de dados pessoais que ocorra em território nacional, ou para efeitos de fornecimento ou fornecimento de bens ou serviços, ou quando os dados pessoais sejam tratados em território nacional. O responsável pelo tratamento é a pessoa singular ou coletiva que toma as decisões sobre o tratamento dos dados pessoais. O operador é uma pessoa física ou jurídica que processa dados pessoais em nome do controlador. Além disso, a LGPD prevê um responsável, pessoa designada pelo controlador para atuar como canal de comunicação entre o controlador, a operadora, o titular dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela proteção de dados. Monitorar e orientar o cumprimento da LGPD.

[…] ainda que para finalidade acadêmica não seja necessário respeitar todo o texto a LGPD, ainda assim, será necessário verificar se o tratamento de dados para fins acadêmica se encaixa também nas hipóteses de tratamento para que seja lícito o seu uso. Aqui a recomendação é documentar a análise e, quando da realização do tratamento de dados, identificar que ele está de acordo com as normas e que o uso é realizado com base em determinado inciso do art. 7º ou 11º […]. (SOLER, 2021, p.32) 3

A segurança de dados no meio acadêmico é um tema cada vez mais relevante e desafiador, dada a crescente produção e compartilhamento de informações científicas e educacionais.

Os dados acadêmicos são um recurso valioso para o avanço do conhecimento, a inovação e a colaboração entre pesquisadores, instituições e sociedade. No entanto, eles também estão

sujeitos a riscos de perda, roubo, vazamento, manipulação ou uso indevido, que podem comprometer a integridade, a confiabilidade e a reputação dos envolvidos.

Por isso, é fundamental adotar medidas de proteção e gestão dos dados acadêmicos, que garantam a sua disponibilidade, confidencialidade e autenticidade. Algumas dessas medidas são: utilizar plataformas seguras e confiáveis para armazenar, processar e divulgar os dados; criptografar os dados sensíveis ou sigilosos; fazer cópias de segurança regularmente; definir políticas de acesso e uso dos dados; obter consentimento informado dos participantes da pesquisa; respeitar os direitos autorais e as normas éticas; e reportar qualquer incidente ou suspeita de violação dos dados.

A gestão e segurança de dados nas instituições de ensino superior são temas de grande relevância e desafio na atualidade. Essas instituições de ensino superior devem se adequar às normas e boas práticas para o tratamento dos dados pessoais de alunos, professores, funcionários e demais envolvidos em suas atividades. Além disso, a pandemia da Covid-19 trouxe novos cenários e demandas para o ensino superior, como a necessidade de adaptação ao ensino remoto emergencial, que implica em novos usos e riscos para os dados pessoais.

A gestão de dados nessas instituições de ensino envolve o planejamento, a organização, o controle e a avaliação dos processos que envolvem os dados pessoais, desde a sua coleta até a sua eliminação. A gestão de dados visa garantir que os dados sejam utilizados de forma adequada, eficiente e ética, respeitando os direitos dos titulares dos dados e os interesses da instituição. A gestão de dados também deve considerar as especificidades do setor educacional, que tem por objetivo instruir e disseminar a cultura de privacidade.

A segurança de dados nas instituições de ensino é um aspecto fundamental da gestão de dados, que visa proteger os dados pessoais contra ameaças internas e externas, como perdas, vazamentos, acessos não autorizados, alterações indevidas, entre outras. A segurança de dados requer a adoção de medidas técnicas, administrativas e jurídicas para

prevenir e mitigar os riscos aos dados pessoais. Também deve-se levar em conta o nível de sensibilidade dos dados tratados, como os dados biométricos ou os dados relacionados à saúde ou à vida sexual dos titulares.

Portanto, a gestão de dados é essencial para garantir o cumprimento da LGPD, a preservação da reputação e da confiança da instituição, a qualidade do ensino e da pesquisa e o respeito aos direitos fundamentais dos titulares dos dados.

Para isso, é necessário que essas instituições realizem um mapeamento dos seus processos que envolvem dados pessoais, nomeiem um encarregado de proteção de dados (DPO), elaborem políticas e procedimentos internos, capacitem seus colaboradores e parceiros, escolham plataformas confiáveis e monitorem constantemente as suas atividades.

[...] Se considerarmos que a LGPD é relativamente nova e que sua entrada em vigor foi postergada em diversos momentos, deveremos assumir que existirão ainda muitos debates acerca da sua aplicabilidade e outros tantos pontos que precisam ser regulamentados e pacificados [...]. (SOLER, 2021, p.199) 3

Por ser uma lei nova e complexa, ela ainda gera muitas dúvidas e discussões sobre como aplicá-la na prática e como regulamentar alguns aspectos que não estão claros na lei. A LGPD também cria a Autoridade Nacional de Proteção de Dados (ANPD), que é o órgão responsável por fiscalizar e orientar sobre o cumprimento da lei.

CAPÍTULO 2

- **Visibilidade da lei e vulnerabilidade dos usuários**

Na era digital atual, a proteção de dados pessoais tornou-se um assunto de extrema importância. Como indivíduos, partilhamos grandes quantidades de informações pessoais online, confiando que serão tratadas com cuidado e respeito.

[...] A relação do direito à autodeterminação informativa (e, nesse sentido, também em boa parte do direito à proteção de dados pessoais) com o princípio da dignidade da pessoa humana, portanto, é, em certo sentido, dúplice, pois se manifesta, tanto pela sua vinculação com a noção de autonomia, quanto com a do livre desenvolvimento da personalidade e de direitos especiais de personalidade conexos, de tal sorte que a proteção dos dados pessoais envolve também a salvaguarda da possibilidade concreta de tal desenvolvimento, para o qual a garantia de uma esfera privada e íntima é indispensável [...] (SARLET, 2021, p. 31 apud SARLET, 2023, p.38)

O trecho aborda a importância do direito à autodeterminação informativa e à proteção de dados pessoais como expressões do princípio da dignidade da pessoa humana. A autora argumenta que esse direito está relacionado tanto à autonomia do indivíduo de controlar as informações que lhe dizem respeito, quanto ao seu livre desenvolvimento da personalidade e aos direitos de personalidade que dele decorrem. Assim, a proteção dos dados pessoais não se limita a evitar o uso indevido ou abusivo dessas informações, mas também a garantir a possibilidade de o indivíduo construir sua identidade e sua esfera privada e íntima. É apresentada uma visão que merece ser lembrada para assim desenvolver uma mentalidade questionadora acerca dos desafios impostos pelas novas tecnologias e pela sociedade da informação.

Deste modo, a confiança tem sido repetidamente desafiada, conduzindo a uma necessidade crescente de regulamentos e leis que protejam os nossos direitos fundamentais à privacidade e à liberdade. A LGPD visa salvaguardar os direitos e a privacidade dos indivíduos em relação aos seus dados pessoais. Estabelece regras e princípios para o tratamento de dados por empresas e instituições públicas, bem como as sanções para eventuais violações.

Um dos desafios significativos enfrentados por ela é a sua visibilidade junto ao público em geral. Muitas pessoas permanecem inconscientes da existência desta lei, dos

seus objetivos e das implicações que ela tem para eles. Consequentemente, não exercem os seus direitos e não cumprem os seus deveres relativamente aos seus dados pessoais. Esta falta de sensibilização também pode se estender a empresas e instituições públicas que não se adaptaram aos novos requisitos, colocando potencialmente os titulares dos dados em risco de violações de privacidade e perdas financeiras. Aumentar a visibilidade da LGPD é crucial para garantir a sua eficácia.

Isto pode ser conseguido através de iniciativas educativas e informativas dirigidas tanto aos cidadãos como aos agentes de tratamento de dados. Tais iniciativas podem incluir campanhas publicitárias, palestras, cursos, folhetos informativos, entre outros meios de chegar ao público. Ao educar os indivíduos sobre os seus direitos e responsabilidades relativamente aos seus dados pessoais, podem tomar decisões informadas e exigir responsabilização das organizações que tratam as suas informações. Além disso, é essencial reforçar os mecanismos de monitorização e fiscalização do cumprimento da lei.

[...] De acordo com Hans Peter Bull, primeiro encarregado da agência federal de proteção de dados alemã, o cerne moral e político das preocupações do Tribunal Constitucional foi (e é) o da garantia da liberdade dos cidadãos em face da repressão por parte do Estado, de modo que a argumentação deduzida na decisão foi orientada de acordo com o objetivo da proteção da liberdade de ação do ser humano, sendo a transparência da coleta de informações um meio para alcançar tal finalidade [...] (BULL, 2009, p. 29 e s apud SARLET, 2023, p.38)

É apresentada uma análise da decisão do Tribunal Constitucional alemão sobre a proteção de dados dos cidadãos. O cerne da questão é o equilíbrio entre a segurança pública e a liberdade individual, que pode ser ameaçada pela coleta e uso de informações pessoais pelo Estado. O autor defende que o Tribunal Constitucional priorizou a garantia da liberdade dos cidadãos, exigindo transparência e limites para a intervenção estatal na esfera privada.

Essa responsabilidade cabe a entidades como a Autoridade Nacional de Proteção de

Dados (ANPD), o Ministério da Justiça Pública, órgãos de defesa do consumidor e organizações da sociedade civil. Ao regulamentar e supervisionar ativamente a aplicação da LGPD, essas entidades podem garantir que as organizações cumpram as disposições da lei, protegendo os direitos dos indivíduos e dissuadindo potenciais violações.

A importância da LGPD vai além da proteção dos direitos dos indivíduos aos dados pessoais. Também busca fomentar o desenvolvimento econômico, social e tecnológico do país. Seus dados são tão valiosos quanto são usados por criminosos que os interceptam. No entanto, quando o roubo de informações ocorre a nível empresarial, pode resultar em enormes perdas financeiras ou mesmo na paralisação das operações. Portanto, é fundamental que a lei seja amplamente divulgada e respeitada por todas as partes envolvidas no tratamento de dados. Isso inclui indivíduos, organizações e instituições governamentais.

[...] Uma das lacunas possivelmente mais importantes não cobertas pelo direito à autodeterminação informativa diz respeito ao fato de que terceiros que acabam tendo acesso aos dados armazenados em algum sistema técnico-informático não se encontram sujeitos às regras sobre a coleta e tratamento de tais dados, de tal sorte que uma das diferenças entre os dois direitos reside na circunstância de que a autodeterminação informativa se refere a um dado ou a um conjunto de dados, ao passo que o direito à garantia da confiabilidade e integridade dos sistemas técnico-informacionais tem por objeto a proteção do sistema como um todo (e por isso a confiança na sua utilização) e os dados em sentido amplo, evitando que terceiros possam se apropriar até mesmo de um perfil da personalidade do usuário dos sistemas [...] (MENKE, 2015, p. 219 apud SARLET, 2023, p.38).

A citação apresenta uma ideia interessante sobre a distinção entre o direito à autodeterminação informativa e o direito à garantia da confiabilidade e integridade dos sistemas técnico-informacionais. Segundo ele, o primeiro direito se refere à possibilidade de o indivíduo controlar os seus dados pessoais que são coletados e tratados por entidades

autorizadas, enquanto o segundo direito se refere à proteção do sistema como um todo e dos dados em sentido amplo, evitando que terceiros não autorizados possam acessar, manipular ou se apropriar desses dados, inclusive de um perfil da personalidade do usuário.

Essa distinção é relevante porque mostra que há lacunas na legislação sobre a proteção de dados que não abrangem todas as situações possíveis de violação da privacidade e da segurança dos usuários dos sistemas técnico-informacionais. Portanto, é necessário que se amplie o escopo do direito à autodeterminação informativa para incluir também o direito à garantia da confiabilidade e integridade dos sistemas técnico-informacionais, ou que se crie um novo direito específico para essa finalidade.

Com relação aos desafios de visibilidade e conformidade persistirão, sem dúvida, à medida que a tecnologia continua a evoluir. Contudo, ao promover continuamente a consciencialização, educar os indivíduos, e reforçando os mecanismos de aplicação, podemos preparar o caminho para uma sociedade mais consciente da privacidade. É através do esforço coletivo de todas as partes interessadas que podemos garantir a proteção dos dados pessoais, promover a gestão responsável dos dados e manter a confiança no ecossistema digital.

Segundo Brandolfo Silva e Bohnenberger (2019), “há sim, vulnerabilidade do consumidor nas redes sociais, e o mesmo tem direitos violados com base no Princípio da Reparação Integral de Danos, que acarreta a responsabilidade objetiva aos fornecedores e prestadores de serviços em benefício do consumidor”. Portanto, é fundamental que os usuários da internet sejam conscientes dos riscos e dos direitos envolvidos no ambiente digital.

A ideia apresentada reflete sobre a vulnerabilidade do consumidor nas redes sociais, que muitas vezes é exposto a práticas abusivas, enganosas ou fraudulentas por parte de fornecedores e prestadores de serviços. O autor evidência que as redes sociais são um

ambiente propício para a violação e lesividade aos seus direitos, pois permitem a disseminação de informações falsas, incompletas ou tendenciosas sobre produtos e serviços, bem como a exposição indevida de dados pessoais dos consumidores.

É proposto, então, algumas medidas para proteger os direitos dos consumidores nas redes sociais, medidas que apesar de simples fazem toda a diferença, mas ainda correm o risco de serem ignoradas, tais como: a fiscalização e a punição dos fornecedores e prestadores de serviços que praticarem condutas ilícitas; a educação e a conscientização dos consumidores sobre seus direitos e deveres; e o incentivo à participação dos consumidores na defesa coletiva dos interesses difusos e coletivos.

A vulnerabilidade de dados é traz alerta uma vez que a segurança da informação é um dos principais desafios enfrentados pelas empresas e indivíduos. Essa vulnerabilidade pode ser definida como qualquer fator que possa contribuir para gerar invasões, roubos de dados ou acessos não autorizados a recursos. Elas incluem, mas não se limita-se, a itens como softwares mal configurados, aparelhos com sistemas desatualizados e arquivos internos expostos publicamente.

Essas falhas de segurança podem surgir tanto por falta de treinamento dos profissionais quanto por uso de soluções de um modo não adequado. Deixar os arquivos expostos publicamente demonstra que as rotinas internas não estão seguindo as boas práticas e resulta em um ambiente que se torna menos confiável. Por exemplo, a manutenção do sistema sem atualizações pode ocorrer devido ao fim do suporte do software ou devido a processos ineficazes de testes e validação de atualizações.

A gestão desses elementos de risco é um processo que traz mais confiabilidade para a infraestrutura de TI. Ela garante que o negócio integre a tecnologia em vários processos sem comprometer sua confiabilidade. Além disso, as empresas podem evitar ataques e, assim, evitar perdas associadas à perda e roubo de dados internos. Sem uma boa gestão de

riscos, integrar a tecnologia ao dia a dia se tornará uma atividade muito mais complexa. Assim os usuários podem se sentir seguros a usar os serviços sem risco de informações pessoais ou de negócios sejam vazadas. Portanto, é importante monitorar e mitigar continuamente possíveis problemas.

Em sintase, a vulnerabilidade de dados é um problema que afeta empresas e indivíduos em todo o mundo. É importante que as entidades e órgãos que administrem essas informações estejam cientes dos riscos e adotem medidas para proteger seus dados e sistemas. A gestão de vulnerabilidades de segurança é um processo fundamental para garantir a confiabilidade da infraestrutura de TI e os protocolos de segurança instituídos que visam evitar prejuízos relacionados à perda e ao roubo de dados.

CAPÍTULO 3

- **Tratamento dos dados pessoais e tutela legal**

Na era digital, a proteção dos dados pessoais tornou-se uma preocupação cada vez mais relevante e premente. Com os rápidos avanços da tecnologia e a utilização generalizada da Internet, as informações pessoais dos indivíduos estão a ser recolhidas, analisadas e partilhadas como nunca antes.

Como resultado, a proteção de dados pessoais, emergiu como uma área vital de consideração legal e ética. A definição de dados pessoais varia entre diferentes jurisdições, mas geralmente se refere a qualquer informação que possa ser usada para identificar um indivíduo, incluindo, entre outros, endereço, nome, endereço de e-mail, perfis de mídia social e número de telefone. Estas informações são recolhidas por numerosos intervenientes, incluindo governos, empresas e até os próprios indivíduos, para cumprir vários fins, tais como prestação de serviços, realização de pesquisas e publicidade direcionada.

[…] Um modo de interpretar essa característica de nossa tradição jurídica está na

perspectiva de ver a proteção jurídica da “privacidade como sigilo” associada a certa proteção do valor da intimidade. Nessa compreensão, o caráter sigiloso de uma informação estaria ligado à qualidade íntima da informação ou da atividade que a gera, o que justificaria a proteção especial conferida pelo ordenamento jurídico a essas informações pessoais para que certas relações de intimidade possam existir. Nessa abordagem, a informação não é íntima e sigilosa apenas se a pessoa a guarda somente para si; ainda pode existir proteção para quem compartilha informações sobre o que faz, sente, pensa e é com certas pessoas de sua escolha e confiança, mas não as compartilha com outros. Afinal, é essa possibilidade que permite relações de intimidade […] (Bioni, 2020, p.598).

O autor destaca que a proteção jurídica da privacidade como sigilo está associada à proteção do valor da intimidade. Nessa perspectiva, o caráter sigiloso de uma informação estaria ligado à qualidade íntima da informação ou da atividade que a gera, o que justificaria a proteção especial conferida pelo ordenamento jurídico a essas informações pessoais para que certas relações de intimidade possam existir. De acordo com essa abordagem, a informação não é íntima e sigilosa apenas se a pessoa a guarda somente para si; ainda pode existir proteção para quem compartilha informações sobre o que faz, sente, pensa e é com certas pessoas de sua escolha e confiança, mas não as compartilha com outros. Afinal, é essa possibilidade que permite relações de intimidade.

No entanto, a recolha e utilização de dados pessoais levantam preocupações significativas sobre privacidade, segurança e autonomia individual. A utilização indevida ou o acesso não autorizado a dados pessoais pode ter consequências graves, que vão desde o roubo de identidade e fraude financeira até à vigilância e discriminação.

[…] na ótica individual como coletiva, importa destacar a ideia da proteção preventiva e consequentemente de medidas judiciais que evitem a lesão de direito extrapatrimonial. O próprio Código Civil, em capítulo sobre os direitos da personalidade, dispõe: “Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem

prejuízo de outras sanções previstas em lei" (art. 12). Na mesma linha, é o caráter preventivo inerente à própria concepção do dano moral coletivo.

Não há necessidade para que o autor – individual ou coletivo – tenha uma efetiva lesão a direito para, num segundo momento, provocar a atuação jurisdicional do Estado. A ameaça a lesão a direito do titular já enseja medidas protetivas, com ampla utilização de todas as providências cautelares previstas no Código de Processo Civil.

Em síntese, a tutela judicial do titular dos dados pessoais abarca todas as medidas preventivas que objetivam evitar a lesão a direito extrapatrimonial, ao lado das providências processuais que buscam reparar (danos materiais) e compensar (danos morais) os direitos violados […] (Bioni, 2020, p.669).

O autor transmite a ideia de que a proteção dos dados pessoais é um direito da personalidade que deve ser resguardado tanto na esfera individual quanto na coletiva, por meio de medidas preventivas e reparatórias. Ele destaca que o Código Civil e o Código de Processo Civil preveem mecanismos para cessar a ameaça ou a lesão a esse direito, bem como para reclamar perdas e danos. Também enfatiza que o caráter preventivo, pois visa evitar que a violação dos dados pessoais cause danos irreparáveis à sociedade.

Reconhecendo estes riscos, os governos de todo o mundo promulgaram legislação e regulamentos para salvaguardar os dados pessoais e proteger os direitos dos indivíduos. Na Europa, o Regulamento Geral de Proteção de Dados (GDPR) estabeleceu um novo padrão global para proteção de dados. O GDPR impõe obrigações estritas às organizações que coletam e processam dados pessoais, incluindo a obtenção de consentimento explícito, a implementação de medidas de segurança e a concessão de direitos aos indivíduos, como acesso, retificação e exclusão de seus dados. O GDPR também aplica pesadas multas por descumprimento, sinalizando a seriedade da proteção de dados.

[…] Para responder a esse acréscimo de risco, nos últimos dez anos (2012-2022), em termos

legislativos, passou-se da não-regulação (de acordo com um entendimento de que os meios virtuais eram meios de plena liberdade) à normatização do ambiente virtual (de acordo com o entendimento mais atual de que a proliferação de condutas ilícitas não pode fazer dos meios virtuais um ambiente favorável à violação de direitos), do descontrole digital ao controle regulado, iniciando-se a tarefa de implantação uma nova fronteira de justiça: a justiça cibernética (cyber justice). Neste meio tempo, a legislação já consolidada (legislação geral) em direitos humanos e em direitos da personalidade veio sendo utilizada, assumida e interpretada como mecanismos de restrição de condutas lesivas em ambiente digital, mesmo inexistindo parâmetros legais específicos (legislação especial). Com esta passagem, opera-se uma importante mudança, substituindo-se a tendência anterior, a da irresponsabilidade, por uma nova tendência, a circunscrição das formas de responsabilidade, implementando-se os meios para repudiar a aparição do ilícito que emprega os meios digitais [...] (Bittar, 2022, p.70).

Neste sentido, as mudanças na legislação adaptam-se aos desafios atuais e oferecem soluções pensadas e com agilidade, permitindo responder ao ritmo dos estímulos trazidos pelas novas tecnologias. A percepção de um descompasso entre o ritmo do direito e o ritmo da tecnologia foi, portanto, reduzida pela adaptação mútua, o que nos permite confirmar que a legislação atual é uma resposta adequada aos problemas levantados pelas novas tecnologias.

No âmbito da transformação gradual da legislação, formou-se gradativamente a quinta dimensão dos direitos humanos, que está em fase de consolidação e desenvolvimento, é o tema do nosso tempo e já atraiu a atenção dos advogados nos últimos anos. A quinta dimensão dos direitos humanos é uma resposta aos desafios da era digital, que exige um novo contorno protetor (que se manifesta na forma de novos direitos) à ideia de dignidade humana.

Além dos requisitos legais, as organizações estão cada vez mais a implementar uma

abordagem de privacidade desde a concepção, em que as considerações de privacidade são integradas na concepção e desenvolvimento de produtos e serviços. Esta abordagem enfatiza a importância de minimizar a recolha de dados, fornece avisos de privacidade claros e transparentes e permitir que os utilizadores façam escolhas informadas sobre os seus dados.

Desse modo, o conceito de tutela de dados pessoais vai além das medidas legais e técnicas. Abrange também considerações éticas, como o respeito pela autonomia e dignidade dos indivíduos.

As diretrizes éticas, como as delineadas por associações profissionais ou órgãos de autorregulação do setor, podem fornecer orientações adicionais e melhores práticas para as organizações garantirem o tratamento responsável dos dados pessoais.

Como indivíduos, também temos a responsabilidade de proteger os nossos próprios dados pessoais. Isto inclui estar atento às informações que partilhamos online, utilizar palavras-passe fortes e exclusivas e rever regularmente as definições de privacidade e segurança em plataformas de redes sociais e outros serviços online. Adicionalmente, mantermo-nos informados sobre as mais recentes práticas de privacidade e proteção de dados pode permitir-nos tomar decisões informadas e responsabilizar as organizações.

Desse modo, a tutela de dados pessoais é de extrema importância no cenário digital atual. À medida que a recolha e a utilização de dados pessoais continuam a crescer, é crucial que tanto os indivíduos como as organizações priorizem a proteção de dados. Isto implica cumprir as leis e regulamentos relevantes, implementar tecnologias e práticas que melhorem a privacidade e promover uma cultura de privacidade e confiança. Somente através destes esforços coletivos poderemos salvaguardar os dados pessoais e defender os direitos dos indivíduos na era digital.

CONCLUSÃO

Em síntese, é apresentado nessa monografia ideias e informações sobre o tema, demonstrado a sua relevância para o meio social e econômico bem como os seus desafios de atuação, que envolve aspectos jurídicos, éticos e técnicos. É preciso garantir que os dados sejam coletados, armazenados e utilizados de forma adequada, respeitando os direitos e as preferências dos titulares. A proteção dos dados pessoais é um direito fundamental dos cidadãos, que deve ser respeitado e garantido pelos agentes públicos e privados que os tratam. Assim, se demostra a importância da Lei Geral de Proteção de Dados, uma legislação que estabelece normas e sanções para os casos de violação da privacidade e da proteção de dados. Além disso, é demonstrado a importância sobre conscientização dos riscos e das medidas de segurança que podem adotar para proteger seus dados pessoais. A segurança de dados pessoais é, portanto, uma responsabilidade compartilhada entre os cidadãos, o Estado e as empresas. Somente assim, será possível construir uma cultura de proteção de dados que beneficie a todos os envolvidos.

REFERÊNCIAS

GUERREIRO, R.; TEIXEIRA, T. Lei Geral de Proteção de Dados Pessoais: Comentada Artigo por Artigo. 4. ed. São Paulo: Saraiva, 2022. E-book.

DONEDA, D.; SARLET, I. W.; MENDES, L. S. Estudos Sobre Proteção de Dados Pessoais. São Paulo: Saraiva, 2022. E-book.

SOLER, F. G. Proteção de Dados: Reflexões Práticas e Rápidas Sobre a LGPD. São Paulo: Saraiva, 2021. E-book.

SARLET, G. B. S.; SARLET, I. W. Série Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação. São Paulo: Saraiva, 2023. E-book.

BIONI, Bruno. Tratado de Proteção de Dados Pessoais. [Digite o Local da Editora]: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em:

https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 21 nov. 2023.

BITTAR, E. C. B.; SARLET, G. B. S.; SARLET, I. W. Inteligência Artificial, Proteção de Dados Pessoais e Responsabilidade na era Digital. São Paulo: Saraiva, 2022. E-book.

BRANDOLFO SILVA, Jose Aparecido; BOHNENBERGER, Gustavo Wohlfahrt. Vulnerabilidade do Consumidor Frente a Manipulação de Dados na Internet. Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/cadernos/direito-do-consumidor/vulnerabilidade-do-consumidor-frente-a-manipulacao-de-dados-na-internet/. Acesso em: 09 nov. 2023.

Forbes Brasil. 'Cibersegurança: entenda os perigos do ambiente digital', 3 nov. 2020. Disponível em: https://forbes.com.br/forbes-tech/2020/11/ciberseguranca-entenda-os-perigos-do-ambiente-digital/. Acesso em: 09 nov. 2023.

Conselho Nacional de Justiça (CNJ). 'Crimes digitais: o que são, como denunciar e quais leis tipificam como crime', 22 jun. 2018. Disponível em: https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/. Acesso em: 09 nov. 2023.

IT EAM. 'Entenda o que é vulnerabilidade de segurança e quais são as mais comuns', 4 maio 2020. Disponível em: https://it-eam.com/entenda-o-que-e-vulnerabilidade-de-seguranca-e-quais-sao-as-mais-comuns/. Acesso em: 10 nov. 2023.

Siteware. 'O que é uma ameaça em segurança da informação?', 3 out. 2022. Disponível em: https://www.siteware.com.br/seguranca/o-que-e-uma-ameaca-em-seguranca-da-informacao/. Acesso em: 10 nov. 2023.

Resumos. 'O que é verificação de vulnerabilidade de banco de dados?', 3 nov. 2023. Disponível em:

https://resumos.soescola.com/glossario/o-que-e-verificacao-de-vulnerabilidade-de-banco-de-dados/. Acesso em: 10 nov. 2023.BBC Brasil. ‘Como megavazamentos de dados acontecem e por que é difícil se proteger deles’, 11 fev. 2021. Disponível em: https://www.bbc.com/portuguese/brasil-56031998. Acesso em: 10 nov. 2023.

---

[1] Acadêmico do Curso de Direito na Faculdade Cerra do Carmo (FASEC).