

**XXXI CONGRESSO NACIONAL DO
CONPEDI BRASÍLIA - DF**

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
III**

IRINEU FRANCISCO BARRETO JUNIOR

PAULO CAMPANHA SANTANA

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydée Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Membro Nato - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

D597

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Irineu Francisco Barreto Junior, Paulo Campanha Santana – Florianópolis: CONPEDI, 2024.

Inclui bibliografia

ISBN: 978-65-5274-063-2

Modo de acesso: www.conpedi.org.br em publicações

Tema: Saúde: UM OLHAR A PARTIR DA INOVAÇÃO E DAS NOVAS TECNOLOGIAS

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3: 2024 : Florianópolis, Brasil).

CDU: 34



XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

O XXXI Congresso do Conselho Nacional de Pesquisa e Pós-Graduação em Direito CONPEDI foi realizado nos dias 27, 28 e 29 de novembro de 2024, em Brasília-DF, e elegeu o tema "Um Olhar a partir da inovação e das novas tecnologias" como eixo norteador dos seus trabalhos. Sob esse escopo, o presente congresso buscou explorar os impactos das inovações tecnológicas no sistema jurídico e nas práticas do Direito, discutindo como as ferramentas digitais estão transformando a pesquisa, a prática profissional e a formação acadêmica na área jurídica.

Saliente-se a enorme aderência entre a temática central do evento e a abordagem do GT Direito, Governança e Novas Tecnologias, um dos mais tradicionais do Conpedi e que, a cada ano, adquire maior centralidade no congresso e no cenário da pesquisa e pós graduação do país. Como de costume o evento propiciou a aproximação entre coordenadores, docentes e pesquisadores de diversos Programas de Pós-Graduação em Direito de todo o Brasil.

A presente edição do Conpedi, dessa forma, abordou o impacto da rápida evolução tecnológica na sociedade, destacando a inovação como essencial para o crescimento e a adaptação em diversos setores. Com foco nas oportunidades geradas por tecnologias como inteligência artificial e big data, especialmente no campo jurídico, o evento também examina os desafios éticos, regulatórios e de acesso que acompanham essas transformações..

Os artigos apresentados GT Direito, Governança e Novas Tecnologias refletem uma ampla diversidade temática que explora as interseções entre tecnologia, direito, ética e sociedade. Diversos artigos destacam o impacto da inteligência artificial (IA) e outras tecnologias emergentes no contexto jurídico, abordando desde a responsabilidade civil e desafios regulatórios até o uso de ferramentas como o ChatGPT na prática jurídica e na proteção de dados pessoais. Destacam-se ainda apresentações exploram os aspectos éticos e econômicos da tecnologia, como biopolítica, biocapitalismo e a monetização de dados pessoais, evidenciando os desafios para a privacidade, integridade corporativa e compliance.

A proteção de direitos fundamentais na era digital, incluindo privacidade, propriedade intelectual e combate à desinformação, também aparece como um tema recorrente. A governança tecnológica é abordada em múltiplas esferas, desde a aplicação de big data na conformidade com a LGPD, até o uso de tecnologia na arrecadação fiscal e no poder

judiciário, com análises institucionais e regulatórias. Em paralelo, pesquisadores analisam o impacto da tecnologia na educação, como a exclusão digital e os desafios para educadores, e a transformação de setores específicos, como a arbitragem desportiva e os ambientes clínicos.

Por fim, destacam-se reflexões sobre democracia digital e participação popular, bem como a valorização do trabalho humano e a relação entre ética algorítmica e integridade corporativa. Esses temas revelam uma preocupação transversal com a construção de uma sociedade tecnológica mais equitativa e ética, com foco na adaptação de instituições e na proteção de direitos em um contexto de acelerada transformação digital.

Os coordenadores responsáveis pelo Grupo de Trabalho cordialmente convidam os interessados a examinar integralmente os artigos em questão, confiantes de que a leitura será proveitosa. Encerramos esta apresentação expressando gratidão pela oportunidade de facilitar os diálogos entre pesquisadores de elevada competência.

Prof. Dr. Irineu Francisco Barreto Junior. Mestrado em Direito da Sociedade da Informação das Faculdades Metropolitanas Unidas - FMU-SP.

Prof. Dr. Paulo Campanha Santana. Mestrado em Direito das Relações Sociais e Trabalhistas do Centro Universitário do Distrito Federal (UDF)

BIG DATA, TENDÊNCIAS E DESAFIOS DA LGPD: IMPACTOS E ESTRATÉGIAS PARA EMPRESAS NA ERA DA PROTEÇÃO DE DADOS

BIG DATA, TRENDS AND CHALLENGES OF LGPD: IMPACTS AND STRATEGIES FOR COMPANIES IN THE DATA PROTECTION ERA

Carlos Alberto Rohrmann ¹
Lucivania de Castro Andrade ²
Fernando Carvalho Carlini ³

Resumo

A formação de big data nas empresas é uma realidade crescente e de importância grande em face da legislação de proteção de dados. Este artigo tem como objetivo analisar os impactos da Lei Geral de Proteção de Dados (LGPD) nas empresas e oferece estratégias para lidar com os desafios associados à conformidade com esta legislação. A pesquisa explora como a LGPD está influenciando a coleta e o processamento de dados, os modelos de negócios e os investimentos em segurança de dados. Além disso, o artigo analisa as oportunidades para melhorar a confiança do cliente e a reputação da marca por meio da conformidade com a LGPD. Por fim, apresenta-se perspectiva para o futuro da proteção de dados e seu impacto contínuo nas empresas, também enfrentado os riscos. Este artigo destaca a importância de uma abordagem proativa para garantir a conformidade com a LGPD e promover uma cultura de privacidade e segurança de dados nas organizações. O trabalho adota a metodologia exploratória e a revisão bibliográfica, utilizando a teoria da arquitetura da rede de Lawrence Lessig como seu marco teórico.

Palavras-chave: Lgpd, Proteção de dados, Impacto nos negócios, Segurança de dados, Teoria da arquitetura da rede

Abstract/Resumen/Résumé

The formation of big data in companies is a growing reality and of great importance in view of data protection legislation. This article aims to analyze the impacts of the Brazilian General Data Protection Law (LGPD) on companies and offers strategies to deal with the challenges associated with compliance with this legislation. The research explores how the LGPD is influencing data collection and processing, business models, and investments in

¹ Advogado em Direito Digital. Doutor em Direito pela Universidade da Califórnia em Berkeley, Estados Unidos da América (2001). Cientista da Computação (UFMG). Mestre em Direito (UCLA). Professor (Mestrado, FDMC).

² Bacharela em Direito (Centro Universitário Ages, 2016); Especialização em Direito Digital e Proteção de Dados (Ebradi, 2022); Graduada em Gestão Comercial (Centro Universitário Ages, 2022); Mestranda em Direito (FDMC).

³ Mestrando em Direito nas Relações Econômicas Sociais pela Faculdade Milton Campos, Bacharel em Direito pela PUC-MG, Pós-graduado em Direito do Trabalho e Previdenciário pela Universidade Gama Filho, Advogado.

data security. In addition, the article analyzes the opportunities to improve customer trust and brand reputation through compliance with the LGPD. Finally, this article presents an outlook for the future of data protection and its continued impact on companies, also facing the risks. This article highlights the importance of a proactive approach to ensure compliance with the LGPD and promote a culture of privacy and data security in organizations. The work adopts an exploratory methodology and a literature review, using Lawrence Lessig's network architecture theory as its theoretical framework.

Keywords/Palabras-claves/Mots-clés: Lgpd, Data protection, Business impact, Data security, Network architecture theory

1. INTRODUÇÃO

A revolução digital transformou profundamente a maneira como as pessoas e as empresas interagem, comunicam-se e conduzem os seus negócios. Essa revolução, embora traga consigo inúmeras vantagens e oportunidades, também levanta preocupações significativas sobre a privacidade e a segurança dos dados pessoais dos usuários quando de seu tratamento pelas empresas. Nesse cenário, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada no Brasil em agosto de 2018, surge como uma resposta crucial para proteger os direitos fundamentais dos cidadãos em meio ao ambiente digital em constante evolução.

A big data com a qual diversas empresas lidam, seja no cadastro de consumidores ou na análise de dados para desenvolver novas estratégias, tornou-se uma realidade crescente e de grande relevância para o campo jurídico, especialmente considerando a legislação de proteção de dados e sua implementação no Brasil. O artigo tem como objetivo analisar os impactos da Lei Geral de Proteção de Dados (LGPD) nas empresas e oferecer estratégias para lidar com os desafios associados à conformidade com esta legislação. Para tal, adota-se uma metodologia exploratória e a revisão bibliográfica.

A LGPD representa um marco legislativo que estabelece princípios, direitos e diretrizes para o tratamento de dados pessoais por organizações públicas e privadas. Ela foi inspirada em regulamentações internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, e visa garantir maior transparência, controle e responsabilidade no uso de informações pessoais.

Para Bioni (2019), “A LGPD é uma peça fundamental no fortalecimento da governança de dados no Brasil. Ela alinha o país aos padrões internacionais de proteção de dados e cria um ambiente mais seguro para negócios e consumidores”.

A crescente preocupação com a proteção de dados pessoais é impulsionada pelo aumento da digitalização em todas as esferas da sociedade. Desde transações comerciais até interações sociais, uma quantidade cada vez maior de dados pessoais é coletada, processada e armazenada por empresas e organizações. Essa abundância de dados levanta questões sobre privacidade, segurança e o potencial uso indevido ou abusivo das informações dos usuários.

O propósito deste artigo é explorar as repercussões da LGPD nas empresas, destacando os desafios e oportunidades que surgem com a conformidade com esta legislação. O artigo analisa como a LGPD está impactando a maneira como as empresas coletam, processam e protegem dados pessoais, além de discutir as implicações legais e as medidas que as empresas

podem tomar para garantir conformidade com os requisitos da LGPD, enfrentando assim os riscos que o armazenamento e o tratamento de dados oferecem (inclusive no que tange aos dados sensíveis).

Para isso, será utilizado como marco teórico a Teoria da Arquitetura da Rede, de Lessig, que se refere ao *design*, à estrutura e à organização de uma rede de comunicação. Seu principal objetivo é definir um *framework* que permita a interconexão de dispositivos e sistemas de maneira eficiente e segura, assegurando a interoperabilidade entre diferentes componentes e tecnologias.

Na era da proteção de dados, integrar a Teoria da Arquitetura da Rede com práticas robustas de conformidade é essencial para as empresas. Ao desenvolver uma arquitetura de rede segura, implementar governança de dados eficaz, promover a conscientização e adaptar tecnologias adequadas, as empresas não apenas garantirão conformidade com a LGPD, mas também fortalecerão a confiança dos clientes, protegerão seus ativos digitais e manterão uma vantagem competitiva no mercado.

2. A LGPD EM FACE DA TEORIA DA ARQUITETURA DE REDE DE LAWRENCE LESSIG

A Teoria da Arquitetura da Rede e a Lei Geral de Proteção de Dados (LGPD) são temas que se interseccionam de maneira significativa, especialmente no contexto da segurança e proteção dos dados pessoais transmitidos e armazenados em redes de comunicação. O artigo pretende explorar como esses dois conceitos se relacionam e como a teoria da arquitetura de rede pode ser aplicada para garantir a conformidade com a LGPD.

A Lei Geral de Proteção de Dados (LGPD) é uma legislação abrangente que estabelece regras e diretrizes para o tratamento de dados pessoais por organizações públicas e privadas no Brasil. Sua finalidade principal é proteger a privacidade e os direitos dos titulares dos dados, garantindo maior controle e transparência sobre o uso de suas informações pessoais. Sua aplicação ao mundo digital é, por um lado, óbvia, e necessária em face da função dogmática do direito digital (Rohrman, 2007); por outro lado encontra desafios típicos do mundo digital, como se verá na apresentação da teoria de Lessig.

A LGPD se aplica a qualquer pessoa natural ou jurídica, de direito público ou privado, que realize o tratamento de dados pessoais (arts. 1º e 3º da Lei nº 13.709/2018). Em seu artigo 5º, a referida Lei dispõe sobre a definição de dados pessoais e tratamento:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (Brasil, 2018, cap. I).

Além do mais, a LGPD estabelece princípios fundamentais para o tratamento dos dados pessoais. Tais princípios visam proteger os direitos fundamentais dos titulares dos dados e garantir que o tratamento de informações pessoais seja realizado de maneira ética, transparente e segura, conforme o artigo 6º:

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;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o

cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Brasil, 2018, cap. I).

Além dos princípios, os direitos dos titulares são fundamentais pois visam garantir que os titulares tenham controle sobre seus dados pessoais e possam exercer sua privacidade e autonomia em relação ao tratamento dessas informações. Estão principalmente descritos no artigo 18 da LGPD.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019)

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019)

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor (Brasil, 2018, cap. III).

As empresas têm uma série de obrigações regidas pela LGPD. Essas obrigações visam garantir a proteção e a privacidade dos dados pessoais que elas tratam. Danilo Doneda, um dos principais especialistas em privacidade e proteção de dados no Brasil, ressalta a importância da LGPD:

A LGPD não é apenas uma norma jurídica, mas uma mudança de cultura em relação ao tratamento dos dados pessoais. Ela representa um avanço significativo na proteção dos direitos dos cidadãos e no estabelecimento de um ambiente mais seguro e transparente (Doneda, 2006).

As obrigações em análise incluem:

a) Nomeação do encarregado de proteção de dados (DPO): empresas que realizam o tratamento de dados pessoais devem nomear um Encarregado de Proteção de Dados (DPO) para atuar como canal de comunicação entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). (Art. 41 da Lei nº13.709/2018);

b) Adoção de medidas de segurança: as empresas são responsáveis por implementar medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Art. 46, da Lei nº13.709/2018).

c) Notificação de incidentes de segurança: as empresas são obrigadas a notificar à ANPD e aos titulares dos dados sobre incidentes de segurança que possam acarretar riscos ou danos aos titulares dos dados (Art.48, da Lei nº13.709/2018).

d) Consentimento: o tratamento de dados pessoais deve ser realizado com o consentimento do titular dos dados ou com base em outras bases legais previstas na LGPD (Art.7º, I, da nº13.709/2018).

Esses são os principais pontos da LGPD que empresas e organizações devem considerar ao lidar com o tratamento de dados pessoais. Mas a legislação também pode impor outras obrigações específicas dependendo do contexto e das atividades de tratamento de dados realizadas pela empresa. Segundo Pinheiro:

A LGPD exige que as empresas passem a ver os dados pessoais como ativos valiosos que precisam ser protegidos e geridos com responsabilidade. A conformidade com a lei não é apenas uma obrigação legal, mas uma oportunidade para as empresas melhorarem seus processos e ganharem a confiança dos clientes (Pinheiro, 2019).

É fundamental que as empresas compreendam esses pontos e adotem medidas para garantir conformidade com os requisitos da LGPD, promovendo assim a proteção da privacidade e dos direitos dos titulares dos dados.

Lawrence Lessig (2006) é amplamente conhecido por sua teoria sobre o impacto da arquitetura na regulamentação, especialmente no contexto da internet. Ele argumenta que a arquitetura (o código) pode regular o comportamento tanto quanto as leis. Quando aplicada à Teoria da Arquitetura da Rede, essa perspectiva pode fornecer insights valiosos sobre como as redes de comunicação e a infraestrutura da internet podem ser projetadas para promover conformidade com regulamentações como a LGPD.

Lessig (1999) argumenta que o conceito de "código é lei" ilustra que a maneira como a tecnologia é projetada pode impor restrições e capacidades sobre o que os usuários podem ou não fazer, semelhante às leis tradicionais. No contexto da internet, a arquitetura da rede pode ser um poderoso regulador de comportamento.

A corrente de Lessig remonta aos anos 1990. Lessig vinha pesquisando à época e publicou alguns artigos sobre o tema. Pode-se destacar o artigo *The limits in open code: Regulatory standards and the future of the net* (Lessig, 1999, p. 795), no qual Lessig trata do código aberto e seus limites no futuro com as grandes empresas usando código fechado. Outro trabalho importante de Lessig foi *The law of the horse: What cyberlaw might teach* (Lessig, 1999, p. 501). Lessig afirma que “*cyberspace is a place, people live there*”, ou “o mundo virtual é um lugar; as pessoas vivem lá” (tradução nossa), em seu trabalho, “*Surveying law and borders: the zones of cyberspace*” (Lessig, 1996, p. 1403), no qual, Lessig argumenta que “*cyberspace is a place, people live there*”, ou “o mundo virtual é um lugar; as pessoas vivem lá” (tradução nossa) e ainda trata da “vida das pessoas no espaço virtual”, afirmando que somos capazes de fazer no mundo online o que se faz no mundo de átomos e até mais. Segundo Lessig: “(...) *while they are in that place, cyberspace, they are also here*”, (Lessig, 1996, p. 1403), ou

seja: “as pessoas, sem deixarem o mundo físico, podem também viver no espaço virtual” (tradução nossa).

Quando se considera a LGPD, a arquitetura da rede desempenha um papel crucial na proteção de dados pessoais. A forma como uma rede é projetada pode facilitar ou dificultar a conformidade com a LGPD.

A teoria de Lawrence Lessig sobre o código como uma forma de regulação oferece uma perspectiva poderosa para entender como a arquitetura da rede pode ser projetada para facilitar a conformidade com a LGPD. Ao incorporar princípios de segurança, gestão de dados, transparência e monitoramento na própria infraestrutura tecnológica, as empresas podem garantir que suas redes não apenas cumpram as exigências legais, mas também protejam os dados pessoais de forma eficaz e eficiente. A arquitetura da rede, portanto, torna-se uma ferramenta fundamental na era da proteção de dados, moldando comportamentos e garantindo a privacidade por meio do design tecnológico.

3. REPERCUSSÕES DA LGPD NAS ATIVIDADES EMPRESARIAIS

A implementação da Lei Geral de Proteção de Dados (LGPD) está causando uma série de repercussões significativas nas empresas, que vão desde a forma como coletam e processam dados até mudanças nos modelos de negócios e investimentos em segurança de dados. Além disso, as empresas enfrentam consequências sérias em caso de não conformidade com os requisitos da LGPD.

As empresas estão sendo obrigadas a revisar e reestruturar seus métodos de coleta e processamento de dados para garantir conformidade com os princípios e diretrizes da LGPD. Isso inclui a necessidade de obter consentimento explícito dos titulares dos dados antes de coletar e processar suas informações, além de garantir que os dados sejam utilizados apenas para as finalidades explicitamente informadas aos titulares.

Empresas que dependem fortemente da coleta e uso de dados pessoais para suas operações podem ser obrigadas a reformular seus modelos de negócios para se adequarem à LGPD. Isso pode envolver a reavaliação de estratégias de marketing, personalização de serviços e produtos, bem como a maneira como os dados são compartilhados com terceiros.

Alessandro Lucchetti, especialista em Direito Digital e Segurança da Informação, comenta sobre a segurança da informação:

A LGPD impõe uma nova perspectiva sobre a segurança da informação. Não se trata apenas de proteger dados contra os ataques cibernéticos, mas de garantir que os dados sejam usados de forma ética e segura em todas as etapas do seu ciclo de vida (Lucchetti, 2018).

As empresas podem precisar investir em novas tecnologias, como sistemas de criptografia e monitoramento de rede, além de desenvolver políticas e procedimentos de segurança de dados mais rigorosos.

As empresas que não cumprem os requisitos da LGPD estão sujeitas a uma série de consequências graves, incluindo multas administrativas que podem chegar a 2% do faturamento da empresa, limitadas a R\$ 50 milhões por infração, segue o artigo correspondente na Lei nº

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

- I - advertência, com indicação de prazo para adoção de medidas corretivas;
- II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- III - multa diária, observado o limite total a que se refere o inciso II;
- IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI - eliminação dos dados pessoais a que se refere a infração;
- X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
- XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
- XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

- I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- II - a boa-fé do infrator;
- III - a vantagem auferida ou pretendida pelo infrator;
- IV - a condição econômica do infrator;
- V - a reincidência;
- VI - o grau do dano;
- VII - a cooperação do infrator;
- VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e

adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019)

§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Redação dada pela Lei nº 13.853, de 2019)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.

§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento (Brasil, 2018, cap. VI, sec. I).

Em resumo, a LGPD está provocando mudanças profundas na forma como as empresas lidam com os dados pessoais dos clientes, exigindo revisões em seus processos, investimentos em segurança de dados e adaptações nos modelos de negócios.

A não conformidade com a LGPD não é apenas uma questão de conformidade legal, mas também representa um risco significativo para a reputação e sustentabilidade das empresas no mercado atual. Para Maldonado, a transparência tem grade relevância em nossa legislação:

A transparência no tratamento de dados pessoais é um dos pilares da LGPD. As empresas precisam ser claras sobre como e por que coletam, usam e compartilham dados, o que aumenta a confiança dos consumidores e fortalece a relação entre empresas e clientes (Maldonado, 2020).

A LGPD trouxe uma série de repercussões significativas para as empresas, tanto no Brasil quanto para aquelas que lidam com dados de cidadãos brasileiros, mesmo que estejam sediadas em outros países (Art.3º da Lei nº 13709/2018). Algumas das principais repercussões incluem:

a) Maior responsabilidade e transparência: as empresas precisam ser mais transparentes sobre como coletam, armazenam, processam e compartilham dados pessoais. Elas também são responsáveis por garantir que os dados sejam utilizados de maneira adequada e que os titulares dos dados tenham controle sobre suas informações.

b) Revisão de políticas e processos internos: as empresas precisaram revisar suas políticas de privacidade, termos de uso e processos internos para garantir que estejam em conformidade com os requisitos da LGPD. Isso inclui a implementação de medidas de segurança da informação e a designação de um encarregado de proteção de dados (DPO) em algumas situações.

c) Investimento em segurança da informação: a LGPD exige que as empresas implementem medidas de segurança da informação adequadas para proteger os dados pessoais contra acessos não autorizados, vazamentos e outras ameaças à segurança.

d) Possíveis sanções por descumprimento: a LGPD prevê sanções para as empresas que descumprirem a legislação, incluindo advertências, multas de até 2% do faturamento da empresa (limitadas a R\$ 50 milhões por infração), suspensão parcial do funcionamento do banco de dados e até mesmo proibição total do tratamento de dados.

e) Aumento da confiança dos clientes: as empresas que demonstram compromisso com a proteção dos dados pessoais de seus clientes podem aumentar a confiança e a fidelidade deles. Isso pode se traduzir em uma vantagem competitiva no mercado.

Além do mais, a Lei Geral de Proteção de Dados (LGPD) e a livre concorrência estão interligadas, especialmente no contexto empresarial, onde ambas podem influenciar e moldar o ambiente de negócios.

Empresas menores podem enfrentar maiores desafios em conformidade com a LGPD devido aos custos associados à implementação de medidas de proteção de dados. Isso pode criar barreiras de entrada para novos concorrentes e reforçar as posições dominantes de empresas maiores, que têm mais recursos para se adaptar à legislação.

Entretanto, empresas que adotam práticas de proteção de dados mais rigorosas e demonstram compromisso com a privacidade dos clientes podem se diferenciar no mercado e ganhar uma vantagem competitiva. Isso pode incentivar outras empresas a seguir o exemplo e aumentar a concorrência com base na proteção da privacidade.

Em outras palavras, diante da nova era digital e da preocupação com a proteção de dados pessoais, torna-se essencial que as empresas possam se adequar às previsões legais da Lei Geral de Proteção de Dados, adotando ações que visem proteger o tratamento de dados pessoais.

4. DESAFIOS E OPORTUNIDADES DA BIG DATA PARA AS EMPRESAS

A implementação da Lei Geral de Proteção de Dados (LGPD) apresenta uma série de desafios significativos para as empresas, ao mesmo tempo em que oferece oportunidades para melhorar a confiança do cliente e fortalecer a reputação da marca.

Segundo Kano e Ramminger (2020), a implementação da LGPD exige que as empresas revisem e ajustem seus processos internos para garantir a conformidade, o que pode ser um desafio significativo devido à necessidade de investimento em tecnologia e treinamento. Abaixo podem-se destacar alguns dos desafios enfrentados pelas empresas na implementação da LGPD:

1. **Complexidade da conformidade:** a LGPD requer uma revisão abrangente dos processos de coleta, armazenamento e uso de dados pessoais, o que pode ser complexo e desafiador para muitas empresas, especialmente aquelas com operações complexas e dados dispersos.
2. **Custos financeiros:** implementar medidas de segurança de dados robustas e garantir conformidade com os requisitos da LGPD pode exigir investimentos significativos em tecnologia, treinamento de funcionários e consultoria jurídica, representando um desafio financeiro para empresas de todos os tamanhos.
3. **Mudança cultural:** adotar uma cultura organizacional centrada na proteção de dados e na privacidade pode ser difícil para algumas empresas, especialmente aquelas que tradicionalmente valorizam a coleta indiscriminada de dados ou que enfrentam resistência interna à mudança.
4. **Gestão de riscos:** identificar e mitigar os riscos associados ao tratamento de dados pessoais, como violações de segurança, vazamentos de dados e não conformidade com os requisitos da LGPD, é um desafio constante que requer uma abordagem proativa e contínua.

A gestão de riscos ainda tem grande impacto quando se trata de empresas que lidam com dados sensíveis, como aqueles relacionados à saúde (Palhares, *et al.*, 2020) setor que ficou muito permeado por várias atividades em face da pandemia da COVID-19, desde 2020 até muito recentemente (Rohrmann, *et. al.*, 2022, p. 57), com destaque para questões de infecções muito sérias quanto ao monitoramento das pessoas doentes, por meio eletrônico (Richards, 2009).

No entanto, Santos (2021) destaca que a conformidade com a LGPD oferece às empresas uma oportunidade de fortalecer a confiança dos clientes e diferenciar-se no mercado ao demonstrar um compromisso com a proteção de dados pessoais.

Ainda nessa linha, de acordo com o relatório da KPMG (2022), a conformidade com a LGPD não apenas ajuda as empresas a evitarem penalidades, mas também pode levar a melhorias na gestão de dados e na eficiência operacional.

Diante disso, como oportunidades das empresas na implementação da LGPD em sua rotina, pode-se destacar:

1. **Construção de confiança do cliente:** a conformidade com a LGPD demonstra o compromisso da empresa com a proteção da privacidade e dos direitos dos clientes, ajudando a construir confiança e lealdade entre os consumidores.
2. **Diferencial competitivo:** empresas que adotam medidas proativas para garantir conformidade com a LGPD podem se destacar no mercado como líderes em proteção de dados, oferecendo aos clientes uma vantagem competitiva significativa.
3. **Melhoria da reputação da marca:** a reputação de uma empresa está intrinsecamente ligada à sua capacidade de proteger os dados pessoais dos clientes. Ao cumprir os requisitos da LGPD, as empresas podem fortalecer sua reputação como defensoras da privacidade e responsabilidade corporativa.
4. **Inovação responsável:** a LGPD promove uma abordagem mais ética e responsável para o tratamento de dados, incentivando as empresas a inovarem de maneira compatível com os valores de privacidade e segurança dos clientes.

O uso da inteligência artificial, que é uma tecnologia muito usada na automação de algumas tarefas específicas que requerem a utilização da inteligência quando os seres humanos as fazem, como por exemplo, jogar xadrez, fazer traduções, resumos ou dirigir veículos (Russell; Norvig, 2022, p. 21), também é usada na inovação do tratamento de dados. A inovação responsável torna-se ainda mais impactante quando se considera o tratamento de dados por algoritmos de inteligência artificial, inclusive com repercussões em dados sensíveis e biométricos, mais uma inovação que ganha muito espaço nesta primeira metade dos anos 2020 (Rover, 2024, p. 52).

Em suma, embora a implementação da LGPD apresente desafios significativos para as empresas, também oferece oportunidades valiosas para melhorar a confiança do cliente, fortalecer a reputação da marca e impulsionar a inovação responsável. Ao abraçar essas oportunidades e enfrentar os desafios de frente, as empresas podem se posicionar de forma mais

competitiva em um ambiente de negócios cada vez mais centrado na proteção de dados e na privacidade.

5. CONSIDERAÇÕES FINAIS

Ao longo deste artigo, analisam-se os diversos aspectos da Lei Geral de Proteção de Dados (LGPD) e suas repercussões nas empresas. Recapitulam-se os principais pontos discutidos e oferecemos sugestões para lidar efetivamente com os requisitos da LGPD, além de considerações sobre o futuro da proteção de dados e seu impacto nas empresas.

A LGPD estabelece regras e diretrizes para o tratamento de dados pessoais, visando proteger a privacidade e os direitos dos titulares dos dados.

A aplicação da Teoria da Arquitetura da Rede é essencial para garantir que as redes de comunicação estejam em conformidade com a LGPD. Isso envolve a implementação de medidas de segurança robustas, a gestão eficaz dos dados, a garantia de transparência e consentimento, e a adesão às melhores práticas de conformidade e governança. Ao integrar esses princípios, as organizações podem proteger melhor os dados pessoais e cumprir os requisitos legais, ao mesmo tempo que mantêm redes eficientes e seguras.

A conformidade com a LGPD requer uma abordagem abrangente que envolve tanto aspectos legais quanto técnicos. A Teoria da Arquitetura da Rede fornece o *framework* necessário para implementar práticas de segurança robustas e eficientes, que são fundamentais para proteger os dados pessoais e garantir a conformidade com a LGPD. As empresas que adotam essas estratégias não apenas atendem aos requisitos legais, mas também fortalecem a confiança dos clientes e melhoram sua posição competitiva no mercado.

A LGPD implica em desafios, como complexidade da conformidade, custos financeiros, mudança cultural e gestão de riscos. No entanto, também oferece oportunidades, como construção de confiança do cliente, diferencial competitivo, melhoria da reputação da marca e inovação responsável.

Pode-se sugerir, diante do estudo, para as empresas lidarem com os requisitos da LGPD como a realizar uma avaliação abrangente dos processos de coleta, armazenamento e uso de dados pessoais, a implementar medidas de segurança de dados adequadas, incluindo tecnologias e políticas de segurança, além de designar um Encarregado de Proteção de Dados (DPO) responsável por garantir a conformidade com a LGPD, estabelecendo procedimentos claros para lidar com solicitações de titulares de dados e incidentes de segurança e fornecendo treinamento regular aos funcionários sobre os princípios e requisitos da LGPD.

A proteção de dados continuará a ser uma prioridade para as empresas, à medida que a digitalização e a interconexão se expandem e a conformidade com regulamentações de proteção de dados, como a LGPD, será cada vez mais exigida e valorizada pelos consumidores.

O artigo, sob uma metodologia exploratória e revisão bibliográfica, adotando Lessig como marco teórico, demonstrou que a tecnologia desempenhará um papel fundamental na proteção de dados, com o desenvolvimento de soluções de segurança e privacidade mais avançadas. Com isso, a ética e a responsabilidade corporativa serão cada vez mais associadas à maneira como as empresas lidam com os dados pessoais dos clientes. Pois, a proteção de dados não é apenas uma questão legal, mas também uma oportunidade para as empresas fortalecerem sua reputação e construírem relacionamentos de confiança com os clientes.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE ANUNCIANTES. **Manual ABA para adequação à LGPD: orientações e boas práticas de governança de dados para Publicitários**. 2020. Disponível em: https://aba.com.br/wp-content/uploads/2020/07/Manual_LGPD_04_junho.pdf. Acesso em: 07 ago. 2024.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A Função e os Limites do Consentimento**. Rio de Janeiro: Forense, 2019.

BRASIL. **Lei n. 12.527 de 18 de novembro de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 07 ago. 2024.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 07 ago. 2024.

CONCI, Milena Loyola; ALBUQUERQUE, Alessandra Lignani de Miranda Starling. A necessidade das empresas se adequarem à Lei geral de proteção de dados pessoais. **Derecho y cambio social**. Disponível em: https://www.derechoycambiosocial.com/revista063/La_necesidad_de_que_las_empresas_cumplan.pdf. Acesso em: 07 ago. 2024.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Renovar, 2006.

KANO, Ricardo; RAMMINGER, Sandra. **LGPD: Lei Geral de Proteção de Dados – Comentários e Análise**. São Paulo: Saraiva, 2020.

KPMG. **Relatório sobre Conformidade com a LGPD: Desafios e Oportunidades**. São Paulo: KPMG, 2022.

LESSIG, Lawrence. **Code and other laws of cyberspace**. Nova Iorque: Basic Books, 1999.

LESSIG, Lawrence. Surveying law and borders: the zones of cyberspace. **Stanford Law Review**. Stanford, vol. 48, n. 5, maio de 1996. Disponível em: <https://www.jstor.org/stable/i252756>. Acesso em: 12 ago. 2024.

LESSIG, Lawrence. The law of the horse: What cyberlaw might teach. **Harvard Law Review**, n. 113, p. 501, 1999. Disponível em: https://cyber.harvard.edu/works/lessig/LNC_Q_D2.PDF. Acesso em: 12 ago. 2024.

LESSIG, Lawrence. The limits in open code: Regulatory standards and the future of the net. **Berkeley Technology Law Journal**, Berkeley, n. 14, p. 759, 1999. Disponível em: <https://dash.harvard.edu/bitstream/handle/1/12918286/The%20Limits%20in%20Open%20Code%20Regulatory%20Standards%20and%20the%20Future%20of%20t.pdf?sequence=1>. Acesso em: 12 ago. 2024.

LESSIG, Lawrence. **Code v. 2.0**. New York: Basic Books, 2006. Disponível em: https://upload.wikimedia.org/wikipedia/commons/f/fd/Code_v2.pdf . Acesso em: 20 ago. 2024.

LUCCHETTI, Alessandro. **Segurança da Informação e Governança de TI**. São Paulo: Brasport, 2018.

MALDONADO, Viviane Nóbrega. **LGPD: Lei Geral de Proteção de Dados Comentada**. São Paulo: Revista dos Tribunais, 2020.

PALHARES, Gabriela. *et al.* **A privacidade em tempos de pandemia e a escada de monitoramento e rastreamento**. Estudos avançados, Ed. 34, 2020.

PINHEIRO, Patrícia Peck. **Direito Digital Aplicado 4.0**. São Paulo: Saraiva, 2019.

RICHARDS, Edward P. Dangerous people, unsafe conditions: The constitutional basis for public health surveillance. **Journal of Legal Medicine**, vol. 30, p. 27, 2009. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1899075. Acesso em: 07 ago. 2024.

ROHRMANN, C. A. The role of the dogmatic function of law in cyberspace. **International Journal of Liability and Scientific Enquiry**, vol. 1, ed 1-2, p. 85, 2007. Disponível em: <https://www.inderscience.com/info/inarticle.php?artid=14583>. Acesso em 07 ago. 2024.

ROHRMANN, Carlos Alberto; MARQUES, B. H.; XAVIER, M. E. P. Inteligência artificial, big data e a vigilância de doentes em face da covid-19 sob a teoria de Edward P. Richards. In: V Encontro Virtual do CONPEDI, 2022, Online. **Direito e Saúde**. Florianópolis: Conpedi, 2022. v. 1. p. 68-85. Disponível em: <http://site.conpedi.org.br/publicacoes/465g8u3r/345136gj/4OYX3On7iQTz4kDA.pdf>. Acesso em: 08 ago. 2024.

ROVER, Aires José. Um panorama bibliométrico da proteção de dados e da privacidade em contexto de avanço da inteligência artificial. **Scire-Representacion Y Organizacion Del Conocimiento**, v. 30, p. 49-58, 2024.

RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: a modern approach**. ed. Kindle, 2022.

SANTOS, Mariana. A implementação da LGPD nas empresas: desafios e oportunidades. **Revista Brasileira de Direito Digital**, v. 3, n. 1, p. 45-68, 2022.

TEIXEIRA, Ilderlândio. **LGPD e LAI**: uma análise sobre a relação entre elas. Serpro. 30 de março de 2020. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2020/lei-acesso-informacao-lai-lei-geral-protecao-dados-pessoais-lgpd>. Acesso em: 07 ago. 2024.