XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS IV

MAIQUEL ÂNGELO DEZORDI WERMUTH

LEONEL SEVERO ROCHA

Copyright © 2022 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

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 - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU – São Paulo
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 - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR – Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade – UNIMAR/FEPODI – São Paulo

Conselho Fiscal:
Prof. Dr. Caio Augusto Souza Lara – ESDHC – Minas Gerais
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. José Filomeno de Moraes Filho – Ceará
Prof. Dr. Lucas Gonçalves da Silva – UFS – Sergipe
Prof. Dr. Valter Moura do Carmo – UNIMAR – São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Daniela Marques De Moraes – UNB – Distrito Federal
Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM – São Paulo
Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie – São Paulo
Comunicação:
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul
Profa. Dra. Maria Creusa De Araújo Borges - UFPB – Paraíba
Prof. Dr. Matheus Felipe de Castro - UNOESC – Santa Catarina
Relações Internacionais para o Continente Americano:
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM – Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
Relações Internacionais para os demais Continentes:
Prof. Dr. José Barroso Filho – ENAJUM
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
Eventos:
Prof. Dr. Antônio Carlos Diniz Murta - Fumec – Minas Gerais
Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC – Paraná
Profa. Dra. Livia Gaigher Bosio Campello - UFMS – Mato Grosso do Sul

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UMICAP – Pernambuco

D597

Direito, governança e novas tecnologias IV [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Leonel Severo Rocha; Maiquel Ângelo Dezordi Wermuth.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-626-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias.

XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS IV

Apresentação

Apresentação

Apresentam-se os trabalhos exibidos, no dia 07 de dezembro de 2022, no Grupo de Trabalho (GT) "Direito, Governança e Novas Tecnologias IV", no âmbito do XXIX Congresso do Conselho Nacional de Pesquisa e Pós-Graduação em Direito – CONPEDI – "Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities" – realizado no campus da UNIVALI em Balneário Camboriú/SC.

O GT, de coordenação dos trabalhos dos Professores Doutores Leonel Severo Rocha e Maiquel Ângelo Dezordi Wermuth, envolveu 20 artigos que, entre perspectivas teóricas e práticas, nos impulsionam à imprescindibilidade da observação dos dilemas da atualidade a partir da ótica do direito, da governança e das novas tecnologias. Os trabalhos apresentados abriram caminho para uma importante discussão, a partir da qual os pesquisadores do Direito puderam interagir, levando-se em consideração o momento político, social e econômico vivido pela sociedade brasileira.

O primeiro trabalho é "DISTÚRBIO DE INFORMAÇÃO: FAKE NEWS E PSICOLOGIA" desenvolvido por Lilian Novakoski e Adriane Nogueira Fauth de Freitas. No referido estudo, os autores analisam o fenômeno das fake news desde a criação da informação falsa até a recepção da notícia pelo leitor. A pesquisa trata da epidemia de informação, traçando comentários voltados a uma economia comportamental e a própria relação do direito com a psicologia.

"EFICÁCIA E APLICABILIDADE DA INTELIGÊNCIA ARTIFICIAL COMO MECANISMO REDUCIONAL DO CUSTO DO PROCESSO JURÍDICO", desenvolvido por Ricardo da Silveira e Silva e Rodrigo Valente Giublin Teixeira trata da aplicação da Inteligência Artificial como instrumento eficaz na redução dos custos processuais e consequente facilitação do acesso à justiça.

Letícia Feliciana dos Santos Cruz, Stephanny Resende De Melo, Victor Ribeiro Barreto são autores do artigo “O DILEMA DAS REDES” E AS TECNOLOGIAS DE VIGILÂNCIA NAS CIDADES GLOBALIZADAS: COMO SE PROTEGER?”, cujo estudo tem como objetivo central a discussão da segurança de dados pessoais pelas empresas.

O tema “SMART CITIES E O USO DE CÂMERAS DE VIGILÂNCIA COM INTELIGÊNCIA ARTIFICIAL E RECONHECIMENTO FACIAL” desenvolvido por Emerson Gabardo e Juliana Horn Machado Philippi tem como objetivo analisar as consequências do uso de câmeras de monitoramento com inteligência artificial e reconhecimento facial no contexto das smart cities, bem como propor regulação para evitar violações a direitos fundamentais.

O artigo de autoria de Pedro Augusto Gregorini e Maria Paula Costa Bertran Munoz, intitulado como “JURIMETRIA APLICADA ÀS DEMANDAS BANCÁRIAS: ESTATÍSTICA DOS TIPOS DE PROCEDIMENTO E ASSUNTOS MAIS FREQUENTES NAS AÇÕES AJUIZADAS PELOS BANCOS NO TRIBUNAL DE JUSTIÇA DE SÃO PAULO”, investiga a proporção de ações em que os bancos são autores no estado de São Paulo e dos tipos de procedimento e assuntos mais frequentes.

De autoria de Lourenço de Miranda Freire Neto, Larissa Dias Puerta de Miranda Freire e Thomaz Matheus Pereira Magalhães, é o artigo “PROTEÇÃO DE DADOS E GOVERNANÇA CORPORATIVA SOCIAL E AMBIENTAL COMO INSTRUMENTOS DE DEFESA DOS TRABALHADORES E CONSUMIDORES”, que parte dos avanços tecnológicos e dos novos meios de comunicação para analisar as dinâmicas das relações de emprego que vem se alterando rapidamente nos últimos anos.

“POSSIBILIDADES PARA UMA GOVERNANÇA GLOBAL: A EDUCAÇÃO COMO INSTRUMENTO DE GOVERNANÇA TRANSNACIONAL”, desenvolvido por Ornella Cristine Amaya e Clovis Demarchi, cuja pesquisa discute o conceito de educação para a era das acelerações.

“OS INFLUENCIADORES DIGITAIS NAS RELAÇÕES DE CONSUMO: CONTRIBUIÇÕES DOUTRINÁRIAS E JURISDICIONAIS SOBRE O TEMA”, é o trabalho de Isadora Balestrin Guterres, Luiz Henrique Silveira Dos Santos e Rosane Leal Da Silva. Os autores analisam como as plataformas digitais são utilizadas por influenciadores – pessoas que exploram sua imagem para divulgar produtos e serviços em seus canais – o que suscita que se questione qual a natureza jurídica de sua atuação e suas responsabilidades em relação ao consumidor.

O artigo “GOVERNO DIGITAL E NOVAS TECNOLOGIAS: ANALISE DA ADOÇÃO DA BLOCKCHAIN NA ADMINISTRAÇÃO PÚBLICA”, desenvolvido por Caroline Vicente Moi, Alexandre Barbosa da Silva e Rahiza Karaziaki Merquides, cujo estudo contextualiza a adoção da BLOCKCHAIN na administração pública, suscitando um aumento da eficiência e na redução de custos quando adotadas pelos entes públicos.

Pedro Henrique Freire Vazatta e Marcos Vinícius Viana da Silva são autores do artigo “DADOS OBTIDOS DAS ESTAÇÕES DE RÁDIO BASE NA CONTRIBUIÇÃO DA INVESTIGAÇÃO CRIMINAL E O DIREITO FUNDAMENTAL À PRIVACIDADE”, que dispõe sobre a proteção da intimidade e da vida privada e a sua respectiva relação com a coleta de dados das estações de rádio base.

“COMPLIANCE NA SOCIEDADE DE RISCO” é o trabalho de Renato Campos Andrade, em que o autor parte da análise dos desafios do compliance na sociedade de risco de Ulrich Beck.

Cibele Andréa de Godoy Fonseca, Emerson Wendt e Ismar Frango Silveira desenvolveram o trabalho “CRIMES CIBERNÉTICOS E SUA PREVISÃO COM USO DE ALGORITMOS DE APRENDIZADO DE MÁQUINA E DE DADOS HETEROGÊNEOS: UM MAPEAMENTO SISTEMÁTICO DE TÉCNICAS DE ANÁLISE E PREDITIVIDADE DE DELITOS”, em que o referido estudo trata do avanço da prática de crimes cibernéticos, suscitando o anonimato de criminosos pelas falhas na persecução criminal na esfera cibernética.

Matheus Adriano Paulo e Márcio Ricardo Staffen explanaram em seu artigo “CONSIDERAÇÕES SOBRE A PROTEÇÃO DE DADOS PESSOAIS COMO UM MECANISMO DE DIREITO TRANSNACIONAL”, acerca da proteção de dados pessoais como um mecanismo de direito transnacional, mencionando o case envolvendo França e Google na política de cookies e no rastreamento/compartilhamento de dados.

“CIBERESPAÇO E O ASSÉDIO A DEMOCRACIA: A CONSTRUÇÃO DE UMA PONTE ENTRE A REGULAÇÃO E A LIBERDADE DE ESCOLHA” é o trabalho de Gustavo Marshal Fell Terra, Marco Antonio Zimermann Simão e Willian Amboni Scheffer, oriundo de pesquisa em que os autores tratam de estudos ligados aos assédios sofridos pela democracia frente às novas práticas virtuais. A análise parte do pressuposto existente entre as regulações atuais e as que surgirão e de que modo esse arcabouço técnico pode influenciar a liberdade na Constituição Federal.

Ranivia Maria Albuquerque Araújo e Lara Jessica Viana Severiano são autores do artigo “A RESPONSABILIDADE CIVIL DECORRENTE DOS ATOS JURÍDICOS PRATICADOS PELOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL”, em que se busca analisar a possibilidade de responsabilização da inteligência artificial.

“INTELIGÊNCIA ARTIFICIAL E VIOLÊNCIA DOMÉSTICA: A GARANTIA À INTEGRIDADE FÍSICA POR MEIO DA RELATIVIZAÇÃO DA PRIVACIDADE” de

Isabelle Brito Bezerra Mendes trata da relativização da proteção de dados diante de situações de violência doméstica e da possibilidade legal de utilização da inteligência artificial como prova nesses tipos de delitos.

“A INTELIGÊNCIA ARTIFICIAL COMO FERRAMENTA PARA TRAZER EFETIVIDADE AO PROCESSO JUDICIAL” de Marcus Jardim da Silva, cujo trabalho trata a inteligência artificial como meio de efetivação da justiça, citando o caso do robô pesquisador.

O artigo “A LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE DO PAPEL DO PODER PÚBLICO NA PROTEÇÃO DOS DADOS PESSOAIS DO CIDADÃO” escrito por Camila Barreto Pinto Silva e Cristina Barbosa Rodrigues, tem por objetivo esclarecer a forma como a administração deverá tratar os dados pessoais diante da LGPD.

“ORGANIZAÇÕES, RISCO E PROTEÇÃO DE DADOS PESSOAIS NA CULTURA DAS REDES: OBSERVANDO O PAPEL DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)” de Ariel Augusto Lira de Moura, Bernardo Leandro Carvalho Costa e Leonel Severo Rocha objetiva analisar o Relatório de Impacto a Proteção de Dados na cultura das redes a partir do questionamento sobre que de pontos pode-se observar de modo a conectá-lo à um contexto maior de transformações da sociedade contemporânea.

O artigo “A AUTORREGULAÇÃO REGULADA DAS PLATAFORMAS DIGITAIS: UMA APROXIMAÇÃO AO COMPARTILHAMENTO DE INFORMAÇÕES” escrito por Fabio Luis Celli, Alfredo Copetti e Sylvia Cristina Gonçalves da Silva analisa a necessidade de regulação das plataformas digitais relacionadas às redes sociais e aos aplicativos de serviços de mensageria privada para o compartilhamento de informações por parte dos usuários.

Agradecemos a todos os pesquisadores da presente obra pela sua inestimável colaboração. Desejamos uma ótima e proveitosa leitura!

Coordenadores:

Prof. Dr. Leonel Severo Rocha – UNISINOS

Prof. Dr. Maiquel Ângelo Dezordi Wermuth - UNIJUÍ

A LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE DO PAPEL DO PODER PÚBLICO NA PROTEÇÃO DOS DADOS PESSOAIS DO CIDADÃO

THE GENERAL DATA PROTECTION LAW: AN ANALYSIS OF THE ROLE OF PUBLIC AUTHORITIES IN THE PROTECTION OF CITIZENS' PERSONAL DATA

Camila Barreto Pinto Silva [1]
Cristina Barbosa Rodrigues [2]

Resumo

A Lei Geral de Processamento de Dados Pessoais (LGPD) regulamentou limites e critérios para tratamento dos dados da pessoa natural e as situações em que a LGPD se aplica à administração pública. O presente trabalho tem como objetivo esclarecer a forma como a administração deverá tratar os dados pessoais e responder às seguintes perguntas: A LGPD se aplica ou não ao poder público? Em que situações? Em caso de vazamento de dados, como a administração pública responde? Para responder aos problemas o artigo será dividido em dois capítulos que compõem o seu desenvolvimento. No primeiro capítulo será feito uma análise dos aspectos gerais da LGPD, passando em seguida, a uma análise da LGPD no Poder Público e qual o papel do Poder Público na proteção dos dados pessoais dos cidadãos. O método de abordagem adotado no desenvolvimento da presente pesquisa é o dedutivo, com base em pesquisa de legislação, jurisprudência, artigos científicos e doutrinas.

Palavras-chave: Lei geral de proteção de dados pessoais, Lgpd, Poder público, Administração pública, Direito fundamental de liberdade e privacidade

Abstract/Resumen/Résumé

The Brazilian General Data Protection Act, known as "LGPD," disciplined the limits and criteria for processing a natural person's data and regulated the situations in which the LGPD applies to the public administration. This paper aims to clarify how the administration should handle personal data and answer the following questions: Does LGPD apply to public authorities or not? In which situations? In case of data leakage, how does the public administration respond? To answer these questions, the article will be divided into two chapters. The first chapter will analyze the general aspects of the LGPD, followed by an analysis of the LGPD in the Public Sector and the role of the Public Sector in protecting citizens' personal data. The deductive method was used in this research, based on research of legislation, jurisprudence, scientific articles, and doctrine.

---

[1] Pós-doutoranda em Direitos Humanos e Tecnologia pela Universidade de Reggio Calabria - Itália. Doutora em Filosofia do Direito e Mestre em Direito pela PUCSP . Advogada e professora na UNIMES.

[2] Doutoranda em Direito Internacional Público pela Pontifícia Universidade Católica de São Paulo - PUC/SP; Mestre em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas - FMU. Advogada e Professora Universitária.

Keywords/Palabras-claves/Mots-clés: General law for the protection of personal data, Gdpr, Public power, Public administration, Fundamental right to freedom and privacy

INTRODUÇÃO

Nossa sociedade vive um momento em que um dos bens mais importantes são os dados pessoais. O valor a eles atribuído, seja em valores monetários ou em detrimento de conhecimento, faz com que seja desejado por empresas públicas e privadas.

A Lei n. 13.709/2018 disciplina a proteção de dados pessoais, do direito da personalidade e do direito fundamental e faz com que a Administração Pública se adapte entre a transparência que rege suas atividades e o regime jurídico de proteção de dados disciplinado na Lei Geral de Proteção de Dados Pessoais (LGPD).

O presente artigo tem como objetivo esclarecer em quais situações a Lei Geral de Proteção de Dados Pessoais se aplica ao Poder Público. Primeiramente realiza uma análise dos aspectos gerais da Lei Geral de Proteção de Dados Pessoais e, em seguida, procede-se a uma análise da aplicação da Lei Geral de Proteção de Dados Pessoais no âmbito do Poder Público e o papel deste na proteção dos dados pessoais dos cidadãos.

A justificativa do presente trabalho se dá, por termos hoje os dados pessoais livres e de fácil acesso, sendo extremamente importantes, seja financeiramente ou para traçar perfil das pessoas, gerando um grande interesse por parte de empresas, órgãos e mídias digitais em seu armazenamento e que sem uma regulação pode ocasionar danos para as pessoas, mas para a sociedade em geral.

O presente trabalho fez uso do método dedutivo, tendo como base para a pesquisa legislação, artigos científicos, jurisprudência e doutrinas.

1. ASPECTOS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS(LGPD)

A Lei Geral de Proteção de Dados Pessoais regulamenta como as entidades públicas e privadas passaram a utilizar os dados pessoais, promovendo uma transformação no sistema de proteção de dados brasileiro.

Inspirada no Regulamento Europeu de Proteção de Dados - GDPR foi aprovada após um longo período de debates para acompanhar as mudanças comportamentais e econômicas

impulsionadas pelas tecnologias de informação e da comunicação, em que o grande pilar é a Internet.

Em virtude de um escândalo de vazamento de dados de usuários do Facebook em razão de coleta de dados pela *Cambridge Analytica* (CA), que acabou interferindo nas eleições dos EUA em 2016 e no plebiscito realizado na Grã-Bretanha para saber se ela continua ou não na União Europeia, também conhecida como *BREXIT*, houve uma grande pressão para a regulamentação do uso dos dados pessoais.

A Lei Geral de Proteção de Dados Pessoais não surgiu para impedir que empresas e organizações coletem dados pessoais, que são informações muito importantes para suas operações, negócios, estratégias de marketing, inovação, pesquisa e políticas públicas entre outras, mas sim, para estabelecer regras visando a segurança de uma sociedade cada vez mais movida a dados, com a padronização de normas e práticas, para promover a proteção de forma igualitária dos dados.

Relativamente à sua vigência, a Lei Geral de Privacidade de Dados Pessoais não se encontra totalmente em vigor. A parte referente às regras gerais entrou em vigor em 18 de setembro de 2020 e as sanções em 1o de agosto de 2021. Por sua vez, a ANPD (Agência Nacional de Proteção de Dados Pessoais) instituída pela Lei n. 13.853, de 8 de julho de 2019, que alterou a Lei n. 13.709/2018 em diversos dispositivos. Sua estrutura e quadro de cargos foi criado pelo Decreto n. 10.474, de 26 de agosto de 2020.

1.1 Fundamentos da Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais é uma lei de proteção e não de vedação, tendo entre os fundamentos explícitos na Lei Geral de Proteção de Dados Pessoais: (i) respeito à privacidade - visando assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada; (ii) autodeterminação informativa - tudo isso está relacionado à proteção dos dados. É o dita os alicerces dessa lei e o cenário. Nas palavras de VAINZOF (2020, p. 20), o *"legislador enxergou no titular dos dados como vulnerável em comparação com os agentes de tratamento"*.

No globo abaixo o SERPRO, uma das maiores empresas de processamento, elenca alguns pontos da lei que entende ser importante para o conhecimento dos cidadãos, a saber: (i) uma regra para todos; (ii) mais para o cidadão; (iii) definição do conceito; (iv) as exceções; (v)

abrangência extraterritorial; (vi) abrangência extraterritorial; (vii) transferência internacional; (viii) fiscal centralizado; (ix) responsabilidade; (x) gestão de riscos de falhas; (xi) transparência; (xii) penalidades rígidas; e (xiii) finalidade e necessidade.



Fonte: Serpro. Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/infografico-lgpd-em-um-giro/@@images/9185dd24-5b70-481e-88b0-7064d14553e5.jpeg. Acesso em: 22 out.2022.

A imagem é bem elucidativa em dispor os pontos importantes tratados pela Lei Geral de Proteção de Dados Pessoais, bem como demonstra a importância do tema, sendo que a lei visa criar um cenário de segurança jurídica, padronizando normas e práticas, visando buscar a

proteção, de forma igualitária, dentro e fora do país, dos dados pessoais dos cidadãos localizados no Brasil.

1.2 Contexto econômico e social

Com relação ao contexto econômico e social em que estão inseridos os cidadãos, o Poder Público e as empresas, observa-se cada vez mais a crescente disparidade nas relações que se estabelece entre os titulares de dados e os detentores das tecnologias da informação e comunicação e o Poder Público.

A ausência de normatização de proteção de dados pessoais ocasionou impactos nas relações empresariais com empresas europeias entre outras, que optaram por escolher Argentina e Uruguai para atuar, uma vez que possuíam regulamentação reconhecidas pela União Europeia.

O Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD) foram implementadas em virtude de escândalos internacionais. Entre eles: (i) as revelações de Edward Snowden sobre atividades de espionagem digital encetado pelo Governo do Brasil, tanto a Presidência da República como relativo à Petrobras; e (ii) o ocorrido com os usuários do Facebook, envolvendo o tratamento ilícito de seus dados por parte da Cambridge Analytica (CA).

Sem a concretização de modelos mais abrangentes para a proteção dos dados pessoais do cidadão, a sociedade estará suscetível há que haja o surgimento de ditaduras digitais, baseadas em tecnologias digitais de vigilância.

Segundo VAINZOF (2020, p. 23)

> A LGPD busca a proteção de direitos e garantias fundamentais da pessoa natural, equilibradamente, mediante a harmonização e atualização de conceitos de modo a mitigar riscos e estabelecer regras bem definidas sobre o tratamento de dados pessoais. Entidades públicas e privadas que enxergarem tais proteções como direitos dos cidadãos e não somente como obrigações a serem cumpridas estarão um passo à frente dessa nova fase do Compliance, que agora, além do combate a corrupção, visa o uso seguro e ético dos dados pessoais.

E ainda, para FILKENSTEIN; FILKENSTEIN (2020, p. 291)

> Para entender a necessidade de uma legislação protetiva de dados pessoais, faz-se necessário entender o ingresso da sociedade em um novo patamar de produção de bens e serviços. Nessa sociedade de informação, a geração, o armazenamento e a transferência das informações são realizados instantaneamente, sendo que as novas

> tecnologias agregam valor à informação. Vale dizer: a informação passou a ser considerada um produto, podendo, inclusive, vir a ser objeto de transações comerciais. Na sociedade de informação há, assim, excesso de informações e riscos relacionados ao uso indevido dos instrumentos computadorizados para desvios ou abusos relacionados aos dados coletados ou armazenados. Nesta realidade, os empresários podem obter informações fundamentais para suas operações cotidianas através da inteligência e do armazenamento de dados.

Haverá um momento em que todas nossas informações estarão à disposição das grandes empresas digitais que poderão antecipar como agiremos ou o que vamos fazer. Cada vez há um maior número de informações coletadas e catalogadas, criando a possibilidade de criar perfis ou mesmo catalogar as pessoas por perfil econômico, pois são importantes e podem trazer vantagens econômicas.

Daí a importância em se garantir um nível aceitável de proteção e de privacidade dos fluxos de dados pessoais dos indivíduos, tanto Nacional como internacionalmente.

2. APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS AO PODER PÚBLICO

Enfim entrou em vigor a tão aguardada Lei n. 13.709/2018, Lei Geral de Proteção de Dados Pessoais – LGPD, que 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.

Norma essencial e extremamente importante para uma sociedade cada vez mais conectada, tem como um de seus fundamentos o respeito à privacidade e a inviolabilidade da intimidade, da honra e da imagem da pessoa e, estabelece boas práticas e procedimentos a serem observados pelos controladores e operadores de dados pessoais no tratamento dessas informações, bem como estabelece sanções para as empresas e entidades públicas que descumprirem essas normas protetivas.

No tocante ao Poder Público, a Lei Geral de Proteção de Dados Pessoais (LGPD), tem uma especial importância, pois sempre fez parte da rotina da atividade dos Poder Público criar, manter e gerir grandes bancos de dados compostos, principalmente, de informações de caráter pessoal dos cidadãos, sobre os quais exercem o seu comando, ou seja, dados pessoais, os quais são utilizados não só para extrair o direcionamento necessário para formulação e execução de

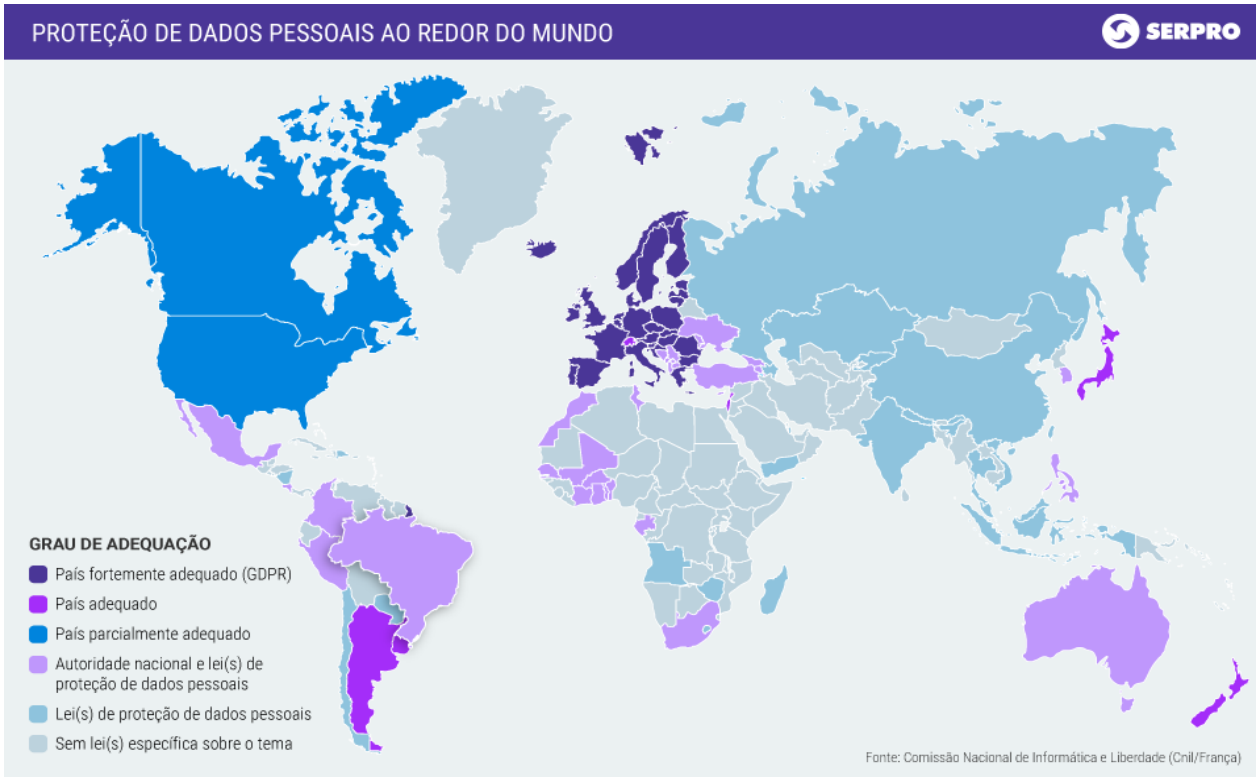
políticas públicas ou para a adequada prestação de serviços públicos, atendendo com mais clareza e efetividade às reais necessidades coletivas com a análise e a devida aplicação dessas preciosas informações que detém, mas o que muitas vezes se observa é o desvirtuamento dessas finalidades, com uso indevido dessas informações para o cerceamento das liberdades individuais em benefício de interesses obscuros.

De fato, com os avanços tecnológicos, redução de custos e o aumento do fluxo diante do ambiente virtual, a coleta, armazenamento e processamento de dados pelo Estado, vem se intensificando e se aperfeiçoando, de forma que as primeiras leis acerca de proteção de dados pessoais, surgidas a partir dos anos 1970 visavam imitar o monitoramento dos cidadãos pelos Estados (CUEVA, 2019).

O tratamento e, principalmente, o uso mercadológico de dados pessoais para formação de perfis de consumidores são muito presentes no setor empresarial, atividades que foram potencializadas e aperfeiçoadas com a coleta dessas informações com a intermediação da internet e de todos seus recursos de processamento, armazenamento e compartilhamento dos mais diversos dados em âmbito global.

Formou-se um cenário de evidente desigualdade nas relações entre os titulares de dados pessoais e empresas, entidades e instituições que coletam e retém com ajuda da tecnologia suas informações, de forma que, sem uma estrutura regulatória de proteção, a sociedade moderna, com o tratamento desses dados, ameaça tirar o bem mais precioso do ser humano, que é a sua liberdade, a sua autodeterminação, sem constantemente monitorado, vigiado ou manipulado em suas atividades, preferências e opções.

Com isso, começou a ser disciplinado ao redor no mundo como, quem e quais situações esses dados pessoais podem coletados e utilizados. Como pode ser visto no mapa abaixo:



Fonte: Serpro (https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais). Acesso em: 22 out. 2022.

É nesse contexto que foi aprovada no Brasil a Lei Geral de Proteção de Dados Pessoais, lei que tem como missão promover um grau aceitável de proteção e de privacidade para os dados dos indivíduos, trazendo, inclusive, regramentos específicos para o Poder Público, posto que este, sob o propósito de zelar pelo interesse público e exercer suas competências legais, é o detentor de um enorme volume de dados, com informações sobre os cidadãos, utilizado especialmente na formulação de políticas públicas, na prestação serviços e atividades públicas.

E de acordo com TASSO (2020, p. 246) temos que:

> A relação jurídica estabelecida entre o Poder Público e o indivíduo titular de dados pessoais é marcada pela assimetria de poder, seja em decorrência da natureza jurídica do ente estatal que atua com poder de império, dotado de poderes para a consecução de seus deveres, como pela circunstância objetiva de que o ente estatal detém grande quantidade de dados pessoais em seus bancos de dados, como insumo ou subproduto do desempenho de sua atividade. É inerente à atividade administrativa a gestão de uma série de bancos de dados potencialmente sensíveis, sendo que a coleta e tratamento desses dados é um ponto nevrálgico em termos de políticas públicas que tenham escala.

Portanto, em decorrência do grande número de dados pessoais que o Poder Público arrecada para cumprir as políticas públicas necessárias ou por conta do poder de império que lhe é característico em determinadas situações, é de fundamental importância o correto armazenamento e tratamento dessas informações.

2.1 Regras de tratamento de dados pessoais pelo Poder Público

A Lei Geral de Proteção de Dados Pessoais estabelece regras específicas para as atividades de tratamento de dados pelo Poder Público e, em seu artigo 23 estabelece que estarão sob sua égide exclusivamente às pessoas jurídicas de Direito Público, ou seja, exclusivamente os (i) órgãos da Administração Pública, direta ou indireta, de qualquer dos Poderes de Estado (Executivo, Legislativo ou Judiciário) e das instâncias federativas (União, Estados, Distrito Federal e Municípios); e (ii) autarquias e fundações públicas constituídas como pessoas jurídicas de Direito Público.

Como bem coloca MORAES, 2021[1] ao dispor que:

> O tratamento de dados pessoais é um aspecto da execução das políticas públicas que mereceu da LGPD regulamentação específica decorrente do reconhecimento de que a massificação das relações travadas entre o Estado e os cidadãos, marcada pela voracidade na coleta de dados, tratados de forma não padronizada e, tampouco, transparente, redunda no risco de o Estado violar direitos e garantias fundamentais do titular.

Portanto, bem colocada a análise quando explica que o tratamento de dados pessoais acaba sendo um dos aspectos de execução das políticas públicas e por isso, mereceu especial atenção por parte da Lei Geral de Proteção de Dados Pessoais.

E como bem colocado por TASSO (2020, p. 246-247) a "atuação do Poder Público é, portanto, excepcional e condicionada". Ou seja, há determinação expressa na lei em quais situações os dados pessoais podem ser tratados pelo Poder Público.

O teor do artigo 23, em seu caput, da Lei Geral de Proteção de Dados Pessoais determina como pressupostos para tratamento de dados pessoais pelo Poder Público: (i) atendimento de finalidade publica; (ii) a persecução de um interesse público; e (iii) e a

[1] Disponível em: https://iapd.org.br/tratamento-de-dados-pessoais-pelo-poder-publico/. Acesso em: 19 jul. 2022.

execução, pelo ente público, de suas competências legais ou cumprimento de suas atribuições. (TASSO, 2020, p.251)

Para que o Poder Público possa tratar dados pessoais dos cidadãos, esses dados devem ser fundamentados por uma base legal legítima. O Poder Público pode atuar nas seguintes atividades, a saber: (i) atividades de segurança pública, (ii) defesa nacional, (iii) segurança do Estado e (iv) atividade de investigação e repressão de infrações penais. Todavia, exclusivamente para esses fins, o tratamento de dados pessoais, possuem regime próprio, expresso no artigo 4º, inciso II da Lei Geral de Proteção de Dados Pessoais, sendo as demais atividades exercidas pelos órgãos públicos seguem a regra de estarem em consonância com a base legal.

Portanto, em detrimento de sua natureza, a Administração Pública não está dispensada da obrigação de proteger os dados pessoais dos cidadãos e em somente utilizá-los de forma legítima. Destarte, a Administração Pública não pode ser excluída da incidência da Lei Geral de Proteção de Dados Pessoais, mas sim, o tratamento de dados pessoais possui regras distintas das aplicadas aos particulares.

Segundo LEVIN (2020, p. 248) "O tratamento de dados pela administração é realizado com uma finalidade pública e, portanto, a incidência do regime jurídico administrativo não pode ser afastada".

Portanto, fica límpido e cristalino que o tratamento de dados realizado pelo Poder Público deve ter finalidade pública e haja a incidência de regime jurídico administrativo.

2.2 Uma análise do papel do Poder Público na proteção dos dados pessoais do cidadão

A Lei Geral de Proteção de Dados Pessoais estabelece expressamente no seu artigo 23, que o Poder Público deverá tratar dados pessoais sem consentimento dos seus titulares, desde que seja utilizado para atender sua finalidade público, na perseguir o interesse público, cumprindo o objetivo de executar as competências legais ou atribuições do serviço público.

Contudo, a Lei Geral de Proteção de Dados Pessoais determina que o Poder Público divulgue nos seus sites e demais meios de divulgação, as hipóteses em que, no exercício de suas competências, é efetuado o tratamento de dados pessoais, mencionando a previsão legal, a

finalidade, os procedimentos e as práticas utilizadas, sendo que os órgãos e entidades públicas também deverão indicar um encarregado de proteção de dados quando estiverem exercendo o papel de operador de dados pessoais.

Nessa toada, é possível concluir das disposições da Lei Geral de Proteção de Dados Pessoais que, embora não seja vedada, há limites para a atividade estatal de tratamento de dados pessoais, a qual deverá sempre estar em conformidade com o interesse público, havendo, entretanto, distinção no nível de cuidados entre os dados pessoais que podem identificar direta ou indireta uma pessoa de uma forma geral e os dados pessoais sensíveis, que são informações formadas por dados mais específicos, relativos à intimidade da pessoa como a sua origem racial ou étnica, opinião política, crença religiosa, saúde ou à vida sexual, havendo para essas informações íntimas mais proteção e rigidez quanto ao seu acesso e tratamento.

Assim, sempre que órgãos e entidades públicas efetuarem o tratamento de dados pessoais no exercício de suas competências legais, vinculadas a políticas públicas e oferecimento de serviços públicos, não será necessário colher o consentimento do titular, porém, deverão informar a finalidade e a forma que esses dados serão utilizados.

Contudo, diante dos diferenciados modos de atuação do Poder Público no exercício da sua missão, a Lei Geral de Proteção de Dados Pessoais definiu formas diferenciadas de incidência das suas regras de acordo com o regime jurídico dos órgãos e entidades públicas.

Destarte, as empresas públicas e sociedades de economia mista por estarem sob a égide de um regime especial híbrido (público e o privado), deverão agir dependendo do caso concreto: se agirem em conformidade com o art. 173, da Constituição Federal, explorando atividade econômica, deverão seguir as normas e ditames definidos pela Lei Geral De Proteção De Dados Pessoais para o setor privado em geral; por outro lado, nos casos em que a finalidade do tratamento for atividade de interesse público, executando políticas públicas, deverão observar as normas da Lei Geral de Proteção de Dados Pessoais direcionadas exclusivamente para o setor público (ROSSO)[2].

[2] https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico-aspectos-gerais-e-desafios. Acesso em 24 jun. 2022.

Desta forma, ante um caso de tratamento de dados pessoais, esses entes precisarão verificar sob qual condição operam, pelas consequências dessa atuação, em regime de mercado ou de direito público, serão distintos.

Além disso, vale mencionar que, considerando suas características peculiares de serviço público exercido mediante delegação, os serviços notariais e de registro, o art. 23, §4º da Lei Geral de Proteção de Dados Pessoais lhes atribui o mesmo tratamento dispensado aos entes públicos quando nas suas atividades tratarem dados pessoais.

O consentimento do titular dos dados pessoais ainda não será necessário para realização de estudos por órgão de pesquisa, com a devida anonimização, ou seja, aplicação de técnicas para impedir a possibilidade de identificação caso sejam utilizados dados pessoais sensíveis.

Assim, de acordo com o artigo 13 da Lei Geral de Proteção de Dados Pessoais, temos que:

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.
> § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.
> § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

O Plenário do Supremo Tribunal Federal, por maioria, acatou medida cautelar em ações diretas de inconstitucionalidade, visando suspender a eficácia da Medida Provisória n. 954/2020, que dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020[3].

[3] Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 15 jun.2022.

Outro aspecto relevante, diz respeito ao tratamento de dados de crianças e adolescentes, o qual apenas poderá ocorrer no melhor interesse destes, mediante consentimento específico e em destaque concedido por, pelo menos, um dos pais ou pelo responsável legal, sendo que os controladores de dados, inclusive o Poder Público, deverão tornar públicos os detalhes acerca dos tipos de dados coletados, da forma de sua utilização e dos procedimentos para acesso às informações tratadas e ainda promover esforços para verificar se o consentimento obtido foi realmente do responsável pela criança. Esse é, portanto, o desafio na coleta de dados pessoais de crianças e adolescentes na atuação estatal, pois o consentimento dos pais ou responsáveis é necessário até mesmo no caso de execução de políticas públicas ou para prestação de serviços públicos, diferentemente do que ocorre com a população adulta.

Vejamos o caso em que o Instituto Brasileiro de Geografia e Estatística (IBGE) identificou crianças sem registros no censo de 2010 na cidade de Bauru, sendo determinado a quebra de sigilo estatístico pelo Tribunal Regional Federal (TRF-3) e posteriormente suspensa a decisão pelo Supremo Tribunal Federal, com base no princípio do melhor interesse das crianças e adolescentes[4].

A única hipótese que dispensa o consentimento dos pais ou responsáveis apenas ocorre quando a coleta for necessária para contatar os referidos responsáveis legais, ou, ainda, para a própria proteção da criança ou adolescente (BRASIL, 2022). Circunstâncias essas que exigem que os dados sejam utilizados uma única vez, sendo ainda vedado o armazenamento, bem como o repasse ou compartilhamento a terceiros.

Dessa forma, para as atividades do Poder Público, assim como para as da iniciativa privada, nas quais sejam desenvolvidas brincadeiras, jogos ou outras atividades dirigidas ao público infanto-juvenil, além do consentimento dos pais ou responsável, a coleta de dados pessoais de crianças e adolescentes deverá restringir-se ao que for estritamente necessário para a realização da atividade proposta (BRASIL, 2022).

Diante dessas medidas assecuratórias estabelecidas pela Lei Geral de Proteção de Dados Pessoais, é ressaltado que o os dados de crianças e adolescentes são um tipo especial de

[4] Disponível em: https://www.conjur.com.br/2017-mai-05/carmen-derruba-ordem-ibge-repassar-dados-criancas-mpf. Acesso em: 15 jun. 2022.

dado pessoal sensível que merecem uma maior proteção, sendo exigido, como regra, o consentimento para o seu tratamento, seja pela iniciativa privada, seja pelo Poder Público.

O Poder Público, por intermédio da ANPD - Autoridade Nacional de Proteção de Dados e demais órgãos com ela relacionados, tem ainda, a missão de requerer a divulgação das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança para a população, de implementar as diretrizes da Lei Geral De Proteção De Dados Pessoais, elaborando Políticas Nacionais de Proteção de Dados, impondo padrões técnicos mínimos para o tratamento dos dados pessoais, fiscalizando a observância dessas normas e diretrizes em âmbito nacional, e aplicando as sanções cabíveis aos infratores, para garantir a proteção dos dados pessoais dos cidadãos, de forma ampla e efetiva.

Dessa forma, fiscalização e a regulação da Lei Geral De Proteção De Dados Pessoais ficarão a cargo da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), que deverá ser um órgão a serviço do cidadão, com missão de servir de canal de comunicação entre sociedade e o Poder Público, permitindo que os cidadãos lhe enviem dúvidas, sugestões, denúncias relativas ao descumprimento das normas da Lei Geral de Proteção de Dados Pessoais para que promova a devida apuração e penalização. A ANPD, tem ainda a atribuição de orientar e apoiar tecnicamente os órgãos de governo e empresas acerca da aplicação da Lei Geral De Proteção De Dados Pessoais nas suas atividades em que há tratamento de dados pessoais.

Diante da modelagem jurídica e operacional adotada pela Lei Geral de Proteção de Dados Pessoais, Poder Público, seus órgãos e entidades, deverão não só cumprir as diretrizes legais de proteção de dados pessoais, mas também, notadamente com a criação de um órgão público especializado, a Autoridade Nacional de Proteção de Dados - ANPD, deverão promover medidas para implementar os novos padrões de proteção e segurança para essas informações, bem como implementar medidas para que essa norma tão importante seja compreendida pela sociedade e efetivamente cumprida.

CONSIDERAÇÕES FINAIS

Como já mencionamos na introdução deste artigo, a nossa intenção foi apresentar como cada vez mais o uso da tecnologia de informação e o tratamento de dados são extremamente importantes para a administração pública e salientamos que a Lei Geral de

Proteção de Dados Pessoais possui um capítulo específico para o tratamento desses dados pessoais.

As mudanças que se farão necessárias para a implementação da referida lei não só deverão respeitar as regras constantes na Lei Geral de Proteção de Dados Pessoais, mas também a Lei de Acesso à Informação, a Lei do Habeas Data e a Lei Geral do Processo Administrativo.

O Poder Público ao armazenar os dados pessoais deverá sempre pensar como será aplicado esses dados para uma melhor execução de políticas públicas com foco no interesse público.

As mudanças organizacionais são muitas vezes complexas e de difíceis implementação, enfrentando enormes desafios institucionais, pessoas e da coletividade para que se concretize tais mudanças.

Concluímos, deixando claro que ao Poder Público é cabível a responsabilidade pelo compartilhamento dos dados armazenados unicamente se forem necessários para a execução de políticas públicas ou em caso de prestação de serviço público.

REFERÊNCIAS

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 jun. 2022

BRASIL. Advocacia-Geral da União (AGU). Casa Civil da Presidência de República; Controladoria Geral da União *et al*. *Guia LGPD - AGU Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD).* 2020. Disponível em: https://repositorio.cgu.gov.br/handle/1/44262. Acesso em: 24 jun. 2022.

CUEVA, Ricardo Villas Bôas. Proteção de dados pessoais no Judiciário. *Revista do Advogado*. São Paulo, Ano XXXIX, nº 144, p. 134-140, nov. 2019.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. PRIVACIDADE e LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. *Revista de Direito Brasileira*, [S.l.], v. 23, n. 9, p. 284-301, fev. 2020. ISSN 2358-1352. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 15 jun. 2022. doi:http://dx.doi.org/10.26668/IndexLawJournals/2358-1352/2019.v23i9.5343.

LEVIN, Alexandre. Tratamento de dados pessoais pelo Poder Público - particularidades previstas na LGPD (Lei n. 13.709/2018). *In*: DAL POZZO, Augusto Neves; MARTINS,

Ricardo Marcondes. (coords.) *LGPD e a administração pública: uma análise ampla dos impactos.* São Paulo: Thompson Reuters Brasil, 2020.

MORAES, Amanda Melo Ditano. Tratamento de Dados Pessoais pelo Poder Público. Disponível em: https://iapd.org.br/tratamento-de-dados-pessoais-pelo-poder-publico/. Acesso em: 19 jul.2022.

ROSSO, Angela Maria. *LGPD e setor público: aspectos gerais e desafios.* Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico-aspectos-gerais-e-desafios. Acesso em 24 jun. 2022

TASSO, Fernando Antônio. *In: LGPD: Lei Geral de Proteção de Dados comentada*. [livro eletrônico]. MALDONADO, Viviane Nóbrega, BLUM, Renato Ópice (coords). 2 ed. rev., atual. e ampl. São Paulo: Editora Thomson Reuters Brasil, 2020. Kindle Edition.

VAINZOF, Rony. *In: LGPD: Lei Geral de Proteção de Dados comentada*. [livro eletrônico]. MALDONADO, Viviane Nóbrega, BLUM, Renato Ópice (coords). 2 ed. rev., atual. e ampl. São Paulo: Editora Thomson Reuters Brasil, 2020. Kindle Edition.

WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. *Revista do Advogado*, São Paulo, Ano XXXIX, n. 144, p. 126-133, nov. 2019.