

LIGA DE ENSINO DO RIO GRANDE DO NORTE  
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE  
CURSO DE DIREITO EM GRADUAÇÃO

VICTÓRIA CHRISTINA JAMES MIRANDA DE OLIVEIRA

**A ADEQUAÇÃO DA ADMINISTRAÇÃO PÚBLICA À LEI GERAL DE PROTEÇÃO  
DE DADOS SOB A ÓTICA DE *COMPLIANCE*, GOVERNANÇA E GESTÃO DE  
RISCO**

NATAL/RN

2023

VICTÓRIA CHRISTINA JAMES MIRANDA DE OLIVEIRA

**A ADEQUAÇÃO DA ADMINISTRAÇÃO PÚBLICA À LEI GERAL DE PROTEÇÃO  
DE DADOS SOB A ÓTICA DE *COMPLIANCE*, GOVERNANÇA E GESTÃO DE  
RISCO**

Trabalho de Conclusão de Curso de Direito  
apresentado ao Centro Universitário do Rio  
Grande do Norte (UNI-RN) como requisito  
final para obtenção do título de Bacharel em  
Direito.

**Orientador(a): PROF(a). ME. LEONARDO  
MEDEIROS JÚNIOR**

NATAL/RN

2023

VICTÓRIA CHRISTINA JAMES MIRANDA DE OLIVEIRA

**A ADEQUAÇÃO DA ADMINISTRAÇÃO PÚBLICA À LEI GERAL DE PROTEÇÃO  
DE DADOS SOB A ÓTICA DE COMPLIANCE, GOVERNANÇA E GESTÃO DE  
RISCO**

Trabalho de Conclusão de Curso de Direito  
apresentado ao Centro Universitário do Rio  
Grande do Norte (UNI-RN) como requisito  
final para obtenção do título de Bacharel em  
Direito.

Aprovado em:

**BANCA EXAMINADORA**

---

Prof. Mestre LEONARDO MEDEIROS JÚNIOR

**Orientador**

---

Prof. Me. ABRAÃO LOPES

**Membro**

---

Prof. Ma. Emanuelli Gondim

**Membro**

Dedico este trabalho à Deus, por ter me capacitado para o crescimento profissional e deste trabalho e a minha família que foram meu alicerce para mais uma conquista.

## AGRADECIMENTO

Agradeço em primeiro lugar a Deus, por todo fôlego e força concedido durante a trajetória dessa conquista.

A família e em especial aos meus avós, Reginaldo James e Maria Regina James, que foram grandes incentivadores, apoiando-me e esforçando-se junto a mim, para que eu suprisse todas elas.

Ao meu namorado, Douglas Lemos, por todo apoio, incentivo, paciência, força e principalmente carinho diante de toda a trajetória até aqui.

Agradeço ao professor Mestre Leonardo Medeiros Júnior que prontamente me orientou, pela paciência e incentivo que tornaram possíveis a conclusão deste Artigo.

As minhas amigas Débora Souza, tão essenciais para orientação profissional e suporte pessoal em toda a trajetória, desde sempre.

Agradeço também a todas as pessoas que estiveram nesse caminho e contribuíram de forma direta ou indireta para esse marco em minha vida.

## RESUMO

O presente trabalho tem como condão principal analisar a adequação da administração pública à Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) sob a ótica de *compliance*, governança e gestão de risco, visto que estabelece conceitos e diretrizes para a implantação no Poder Público, devendo ser referência quanto a aplicabilidade e desenvolvimento. Para atender ao objetivo do presente trabalho, baseia-se na exploração da legislação vigente, de modo a complementar o que está estabelecido na LGPD, além de fazer uso de doutrinas que versam sobre a Responsabilidade Civil, LGPD, *Compliance* e o Poder Público, para uma melhor compreensão e interpretação do assunto abordado. Constatou-se que, a LGPD é de vital importância para a sociedade em geral, e em especial para o Poder Público, porém para sua efetividade, faz-se necessário atrelar a estratégias de gestão risco e mapeamento de processos vinculado ao engajamento dos agentes de proteção de dados no Brasil.

**Palavras-chave: LGPD. Responsabilidade Civil. Dados Pessoais. Compliance. Gestão de Risco.**

## **ABSTRACT**

The main feature of this work is to analyze the adequacy of public administration to the General Data Protection Law – LGPD (Law nº 13.709/2018) from the perspective of *compliance*, governance and risk management, since it establishes concepts and guidelines for the implementation in the Public Power, and should be a reference regarding applicability and development. To meet the objective of the present work, it is based on the explanation of the current to complement what is established in the LGPD, in addition to making use of doctrines that deal with Civil Liability, LGPD, *Compliance* and the Public Power, to a better understanding and interpretation of the subject addressed. It was found that the LGPD is of vital importance for society in general, and in particular the Public Power, but for its effectiveness, it is necessary to connect to risk management strategies and mapping of processes connected to the commitment of security agents data protection in Brazil.

**KEYWORDS:** LGPD. Civil Responsibility. Personal Data. *Compliance*. Risk Management.

**Sumário**

<b>1. INTRODUÇÃO</b>	<b>9</b>
<b>1.1. LEI GERAL DE PROTEÇÃO DE DADOS</b>	<b>12</b>
2.1. PERSPECTIVA HISTÓRICA	12
2.2. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS	14
2.3. FUNDAMENTOS E PRINCÍPIOS	15
2.3.1. PRINCÍPIO DA FINALIDADE	17
2.3.2. PRINCÍPIO DA ADEQUAÇÃO	18
2.3.3. PRINCÍPIO DA NECESSIDADE	18
2.3.4. PRINCÍPIO DO LIVRE ACESSO	18
2.3.5. PRINCÍPIO DA QUALIDADE DOS DADOS	18
2.3.6. PRINCÍPIO DA TRANSPARÊNCIA	19
2.3.7. PRINCÍPIO DA SEGURANÇA	19
2.3.8. PRINCÍPIO DA RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS	19
<b>2.4. A RELAÇÃO ENTRE A LEI DE ACESSO À INFORMAÇÃO E A LGPD</b>	<b>20</b>
<b>3. A LGPD, COMPLIANCE E GOVERNANÇA NA ADMINISTRAÇÃO PÚBLICA</b>	<b>21</b>
3.2. BOA GOVERNANÇA	22
3.3. COMPLIANCE	24
<b>4. IMPLEMENTAÇÃO DA BOA GOVERNANÇA</b>	<b>26</b>
<b>5. CONSIDERAÇÕES FINAIS</b>	<b>27</b>
<b>REFERÊNCIAS</b>	<b>28</b>

## 1. INTRODUÇÃO

As últimas décadas foram marcadas por rápidas e constantes transformações nas concepções no que tange o modelo econômico aliado aos avanços tecnológicos, trazendo novos e complexos desafios quanto ao uso de dados pessoais captados. Em meio à Quarta Revolução Industrial, Lévy (2001, p. 24) afirma que se vive em um império não territorial, ou seja, existe um ponto central, que é virtual, e que faz sentir a sua influência por toda parte.

Os dados pessoais são indispensáveis e usufruí-los sem uma norma específica na regulamentação de seu manuseio, geraram recorrentes abusos, passando a serem perceptivos como verdadeiras minas de ouro, visto que, sabendo-se interpretar suas informações, tornam-se ferramentas valiosas para a organização de estratégias de mercado. Isto é, quanto mais dados obtidos pelas empresas, mais assertivas elas terão no que diz respeito à experiência vivida por seu cliente. Logo, quem tem informação, tem poder!

Como consequência do uso desenfreado desses dados, desenvolveu-se o conceito de privacidade e segurança dos dados sob a perspectiva de violação de Direitos, por vezes irreversíveis. Tem-se essa realidade fortemente praticada nas grandes plataformas, onde Frank Pasquale (apud FRAZÃO, 2019, p. 42) resume de maneira contundente a forma com que os dados pessoais são tratados pelas mesmas. “No seu livro, *Turing’s Cathedral*, Jorge Dyson afirma que o Facebook define o que somos, a Amazon define o que queremos e o Google define o que pensamos”.

Numa visão do plano político internacional, um grande exemplo que pode ser citado dos riscos do uso desenfreado e compartilhamento de dados pessoais são as denúncias de coleta e tratamento abusivo, bem como a suspeita de manipulação ocorrida nas eleições americanas de 2016, apesar de inexistentes as evidências concretas de que o *Facebook* e a *Cambridge Analytics* tenham interferido no resultado das eleições presidenciais dos Estados Unidos da América (EUA).

Nesse contexto, a União Europeia (UE) possui, desde 1995, regulamentação da obtenção, guarda e uso proteção de dados, conhecido como *General Data Protection Regulation* (GDPR) e, posteriormente, promulgou o Regulamento Geral de Proteção de Dados Europeu nº 679, aprovado em 27 de abril de 2016, cujo objetivo era de "harmonizar a defesa dos direitos e das liberdades fundamentais das

peças singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros”.

Essa medida possibilitou a restrição dos países que mantinham relações comerciais com a Europa, obrigando-os a promulgar normativas com conteúdo adequadas ao regulamento europeu. tendo em risco encarar alguma dificuldade comercial junto aos países membros da União Europeia, a exemplo da impossibilidade de receber dados pessoais dos cidadãos europeus, por não terem nível correspondente de proteção de dados.

No Brasil, após diversas experiências da autorregulação dos dados pessoais pelo mercado demonstraram ser insuficientes, e diante de um cenário de debates acerca da titularidade e da forma com que os dados pessoais são tratados não só pelas empresas mas também pelos governos, após uma década de estudos foi aprovada, 14 de agosto de 2018, a Lei nº 13.709 - Lei Geral de Proteção de Dados (LGPD), grande avanço onde, de forma multissetorial e extraterritorial, e alcançando as iniciativas público-privadas, buscou-se regulamentar o uso dos dados.

A lei brasileira é focada na proteção dos dados de pessoas, protegendo os direitos fundamentais da liberdade de expressão, privacidade e o livre desenvolvimento da personalidade da pessoa natural (artigo 1º e 2º). Assim, não houve restrição ao meio virtual, mas sim a todos os meios que permitam a obtenção voltada ao mau uso dos dados individuais.

Sob essa perspectiva, ao tratarmos da iniciativa pública, inicialmente é importante frisar os conceitos do Direito Administrativo, sendo este submetido a diversas hipóteses de atuação na administração pública tanto nos regimentos jurídicos tipicamente de direito público, quanto nas normas proveniente majoritariamente do direito privado. Entretanto, ressalvadas as hipóteses constantes de inaplicabilidade da lei prescrita nas alíneas “a” (segurança pública), “b” (defesa nacional), “c” (segurança do Estado) ou “d” (atividades de investigação e repressão de infrações penais) do inciso III de seu artigo 4º, a LGPD é aplicável de pleno direito.

A Administração Pública, devido às suas natureza e finalidade, detém e trata quantidade expressiva de dados. Desde o final do século XX, a adaptação por parte do Poder Público a fim de operacionalizar bem como a atuação de gestores públicos estão cada vez mais alinhados ao uso da grande quantidade de dados coletados e processados, tornando-se uma Administração Pública orientada por dados.

Nesse sentido, a temática de “Tratamento de Dados Pessoais pelo Setor Público”, em seu Capítulo IV da Lei 13.709/2021 (Lei Geral de Proteção de Dados Pessoais) apresenta, com exclusividade, a condução de execução e/ou cumprimento do tratamento de dados pelo setor público.

Insta destacar que, há particularidades que devem ser observadas sob à Lei de Acesso à Informação (LAI), tendo como base o art. 23 da LGPD “O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011”. A LAI relata em seu artigo 1º que “I - órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios”.

Sendo assim, uma vez que a Administração Pública poderá tratar e usar de forma compartilhada os dados pessoais necessários à execução de atividades de interesse público e, ainda no § 1º do artigo 26 e 27, haja vista que lhe é permitida a transferência e o uso compartilhado de dados pessoais coletados pelo Poder Público a pessoas jurídicas de direito privado quando houver a delegação do serviço público e da atividade pública ao particular, principalmente no tocante às contratações públicas. Surgindo, dessa forma, questionamentos ao que se refere à amplitude e ao limite da eficácia normativa frente aos princípios administrativos basilares, previstos no artigo 37 da Constituição Federal/1988, bem como o dever da licitação sendo esta uma regra constitucional imposta às contratações públicas, previstas no inciso XXI deste mesmo artigo (BRASIL, 1988, 2018a; MEDAUAR, 2018; SCHRAMM, 2020).

Vale destacar um ponto de extrema importância é que a LGPD tornou indispensável o cumprimento dos princípios estabelecidos no “*Privacy By Design*” e “*Privacy By Default*”, os quais visam permitir a adequada governança de dados, seja através de produção de aplicativos e/ou recursos digitais dentro do contexto da proteção de dados. Por isso, a adoção das boas práticas e da governança através da gestão de riscos tem por finalidade aperfeiçoar as atividades, estimular a inovação, assim como mitigar riscos relativos a incidentes de segurança envolvendo dados pessoais, além de gerar confiança entre o titular e os agentes de tratamento.

A metodologia aplicada neste trabalho é de cunho essencialmente bibliográfico, baseando-se na pesquisa em livros, periódicos, jurisprudência e artigos consultados na internet.

Para propiciar um melhor entendimento, esta pesquisa tem por finalidade analisar a implementação da LGPD na Administração Pública e nos instrumentos contratuais celebrados por meio dos processos licitatórios vigentes, de modo a assegurar que seus fornecedores estejam em consonância às práticas estabelecidas na referida lei e ao Estado, haja vista a problemática reside no aspecto do equilíbrio entre as normas que regem a Administração Pública, a exploração econômica e a proteção dos titulares dos dados.

## **1.1. LEI GERAL DE PROTEÇÃO DE DADOS**

### **2.1. PERSPECTIVA HISTÓRICA**

Promulgada em 14 de agosto de 2018, a Lei Geral de Proteção de Dados (Lei nº 13.709), doravante apenas de LGPD, se situa como um meio de efetivação dos direitos da personalidade (COELHO, 2019), uma vez que, é considerada por muitos, um marco para a história da Administração Pública no Brasil por resultar em efetivas ações a fim de evitar o uso indevido dos dados coletados.

Posto isto, a governança pública possui um papel fundamental e de referência, principalmente no que visa assegurar a atuação de órgãos e/ou entidades públicas para que estejam orientadas em suas ações com princípios éticos, focados no bem estar dos cidadãos e promoção de tratamentos igualitários.

No Brasil, antes da publicação da Lei nº 13.709/2018, existiam leis setoriais acerca do assunto, mas que formavam uma “colcha de retalhos”, como destaca Bruno Ricardo Bioni (2019).

Iniciando com o Código de Defesa do Consumidor (CDC), Lei nº 8.078 de 11 de setembro de 1990, a qual disciplina sobre os bancos de dados e cadastros de consumidores, em seu artigo 43, assegurando ao consumidor “... acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes”.

Posteriormente, o Código Civil de 2002, Lei nº 10.406 de 10 de janeiro de 2002, também se envolve na temática mas, aproximando-se das preocupações mais atuais dos direitos da personalidade - âmbito da constitucionalização do Direito Civil

(GODINHO, 2013), estabelece as bases da proteção à personalidade. Insta destacar também, a Lei de Cadastro Positivo, Lei nº 12.414 de 09 de junho de 2011, cujo objetivo é regulamentar o disposto no CDC.

Um momento de relevância até a promulgação da LGPD, foi a aprovação do Projeto de Lei nº 4.060/2012

A Lei nº 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionadas ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionadas às pessoas (PINHEIRO, p. 15).

De modo geral, a LGPD institui regras a todas as pessoas jurídicas, privadas e/ou públicas, para o uso dos dados atribuídos à titularidade dos dados à pessoa física, objetivando a proteção das mesmas e de seus direitos fundamentais garantidos na Constituição Federal, tais como liberdade, privacidade e livre desenvolvimento, dentre outros.

Apesar de todo o avanço e desenvolvimento tecnológico em ritmo acelerado, a LGPD não se restringe ao ambiente virtual. As novas tecnologias de transmissão, coleta, armazenamento e processamento de dados tanto *online* quanto no *off-line*, possuem limitações estruturais relevantes as quais a tornam menos rentáveis e atentatórias aos direitos fundamentais tutelados. Tal temática possui tanta relevância que será acrescida na Constituição Federal, já aprovada pelo Congresso Nacional, representando o compromisso do Governo em garantir o respeito à privacidade dos cidadãos para a garantia do direito fundamental.

Vale ressaltar que, essa captação de dados é de extrema relevância para a eficiência econômica, ao passo que foram possíveis a produção e a divulgação dos produtos fossem mais efetivas. Desta forma, quanto mais informações sobre o consumidor fosse captada pela empresa, menor seria a sua capacidade de escolha foi sendo suplantada pelos interesses das grandes corporações.

Todo o processo do desenvolvimento legislativo referente à proteção dos dados pessoais serviu para que o Brasil estivesse alinhado com os países mais

avançados na temática, como a União Européia, Japão, Estados Unidos e Argentina.

A regulação europeia de proteção de dados (*General Data Protection Resolution* - GDPR) à LGPD foi o primeiro instrumento normativo específico sobre o assunto, incluindo no seu texto critérios para a manutenção dos fluxos de dados. Dessa forma, era necessário que, países interessados em participar do ciclo de dados com entidades europeias, comprovasse que possuem legislação própria, com condições mínimas de segurança e garantias de proteção desses dados.

Essas exigências da UE referente ao compartilhamento de dados, permitiu que a LGPD tramitasse no Congresso Nacional, sendo agilizada pela necessidade do mercado nacional em demonstrar compatibilidade com a legislação europeia para dar continuidade a suas atividades.

No Brasil, o Poder Público como sendo o maior detentor de dados, é definido pela LGPD de maneira ampla e inclui órgãos ou entidades dos entes federativos e dos três Poderes. Desse modo, a implementação deve ocorrer não apenas em empresas privadas, mas também pela Administração Pública, sendo este o maior exemplo, sendo previsto no art. 55-J, XI e XVI da Lei que a Associação Nacional Proteção de Dados (ANPD) poderá solicitar informações específicas sobre o âmbito, a natureza dos dados e outros detalhes envolvidos na operação, por meio de auditorias, passíveis de sanções, conforme estabelecido no art. 52, § 3°.

## 2.2. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A partir da promulgação da LGPD, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), cuja competência está estabelecida pelo art. 55-J da Lei 13.709/2018 (Lei Geral de Proteção de Dados), tendo como principais funções o zelo pela aplicação da legislação, a fiscalização, comunicação com os controladores e a fixação de sanções, caso verificadas irregularidades.

Por ainda não possuir autonomia, uma vez que está vinculada à Presidência da República, é composto pelo Conselho Diretor, Corregedoria, Ouvidoria, órgão de assessoria Jurídica, unidades necessárias à aplicação da LGPD e um Conselho Nacional, sendo este último um importante instrumento para a democratização da lei proveniente de sua função está diretamente ligada a atuar junto à sociedade para a divulgação de informações de realizações de ações afirmativas.

As aplicações das sanções e penalidades pela ANPD deverão levar em consideração os parâmetros fixados em lei, no art. 52, §1º, os quais estabelecem desde advertências até multas com limites de R\$50.000.000,00 (cinquenta milhões de reais).

### 2.3. FUNDAMENTOS E PRINCÍPIOS

Assim como toda norma, a LGPD é baseada em princípios e regras, sendo apresentados nos 65 artigos, divididos em dez capítulos, estes divididos em seções. A princípio, delimita-se os limites de aplicação, territorialidade, conceitos e princípios. Entretanto, de modo geral, em primeiro plano há a especificação de quais são seus objetivos de forma clara, suas funções de apresentar ao intérprete o que se persegue com este diploma a fim de pavimentar o caminho e depois dispor sobre como se deve chegar ao objetivo.

Em razão disso, o artigo 2º da mesma lei traz um rol de fundamentos, incluindo:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - à inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Sob esse viés, tais fundamentos servem de base para a interpretação de todos os dispositivos da lei e resguardam a relação com os direitos fundamentais da Constituição Federal. E, assim, materializando alguns direitos e garantias fundamentais da constituição, a lei procurou equilibrar os direitos individuais com as situações nas quais o interesse público deve prevalecer.

Observando o primeiro fundamento disposto neste artigo, em seu inciso I, forma-se uma total harmonia com o inciso X do art. 5º da constituição, o qual decreta a regra geral da inviolabilidade da intimidade e vida privada, replicado no inciso IV do mesmo artigo da LGPD. Desse modo, percebe-se então que está relacionado a uma das bases do Estado Democrático de Direito, ou seja, o respeito ao indivíduo.

A autodeterminação informativa definida como o segundo fundamento da LGPD nos demonstra que o titular de dados deve ter controle sobre os mesmos, tendo consciência de como seus dados são coletados, com qual intuito e a quem terá acesso a tais informações, dando poder de decisão em consentir ou não.

Em consonância, a lei prevê no inciso X, do art. 5º, um conceito ampliado de tratamento, os quais' abarcam diversas operações realizadas com dados pessoais, quais sejam:

“Art. 5º [...] X - 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.”

Em seu inciso III, a lei compreende que o mau uso dos dados do titular pode levar à violação destes direitos, que também encontra razão nos direitos constitucionais.

Desse modo, observa-se que os primeiros fundamentos reúnem um conjunto de problemáticas voltadas para a proteção do indivíduo, de modo a até captar enunciados constitucionais. Em contrapartida, a segunda parte, a partir do inciso V, busca sanar questões mais complexas ao Estado Democrático de Direito, ao que tange os direitos que prezam pelo livre desenvolvimento do indivíduo na esfera da economia.

Nessa perspectiva, essa segunda parte, composto pelos incisos V e VI, referenciam a preocupação do legislador com a livre iniciativa e o desenvolvimento econômico do país que, mesmo com a intervenção com o objetivo de proteção aos dados pessoais, faz-se necessário reconhecer a magnitude dos avanços tecnológicos e da livre iniciativa para o desenvolvimento da sociedade.

Restringe-se à observância de princípios específicos de modo a garantir a regularidade do tratamento de dados levado a cabo pelos agentes de tratamento. Disposto no artigo 6º da Lei, elenca 10 princípios, sendo destacados os princípios da “segurança”, “prevenção” e da “responsabilização e prestação de contas”. Isso permite que os agentes de tratamento de dados exijam o limite necessário para a

operacionalização de suas finalidades e que sejam adotadas medidas técnicas e administrativas.

Isto posto, a LGPD representa uma nova fase do *compliance*, promovendo um tratamento ético dos dados pessoais, levando em consideração os fundamentos e premissas da lei, ao intento de assegurar os direitos fundamentais da liberdade, da privacidade, da intimidade, e do livre desenvolvimento da personalidade da pessoa natural.

Os princípios são elementos indispensáveis para que haja a interpretação dos textos legais condizente com a realidade prática em sociedade. Mas sem a ponderação de seu uso, tornam o propósito da norma apenas ideológico, o que dificulta sua aplicação devido não haver diretrizes claras no que diz respeito ao seu objetivo. Por essa razão, define Robert Alexy, *in verbis*:

Princípios são, por conseguinte, mandamentos de otimização, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas (ALEXY, 2006, p. 90).

Na LGPD, os princípios elencados pelo legislador, estão explicitados a fim de que não restassem dúvidas sobre a metodologia necessária na sua aplicação. Assim sendo, os mesmos estão enumerados nos incisos do art. 6º da LGPD, fazendo necessário analisá-los alguns de forma breve e individual.

### 2.3.1. PRINCÍPIO DA FINALIDADE

Este princípio tem como finalidade determinar a força do que é pactuado entre as partes, dando ao titular dos dados a prerrogativa de poder analisar o que será coletado e se há razão de ser. Dessa forma, há a garantia de que os tratamentos dos dados não serão desvirtuados sem que haja expressa autorização do titular para a finalidade a qual foi feita a coleta.

Assim, o controlador e operador estão submetidos a uma obrigação restrita, e previamente pactuada, de modo que os controladores devem ter bem definidos, desde a concepção do projeto, para qual finalidade será utilizada os dados.

### 2.3.2. PRINCÍPIO DA ADEQUAÇÃO

O princípio da adequação está diretamente ligado ao princípio da finalidade, pois estabelece que deve ser observada para evitar abuso no tratamento dos dados pessoais.

Tem como principal finalidade, em casos de questionamento pelo titular, identificar que os dados estão sendo coletados e tratados para além daquilo que foi ora pactuado, para que caso o controlador alargue a finalidade a que se destina a coleta de dados e realize um novo tratamento ou cesse ou dados para empresas com fins não previstos.

### 2.3.3. PRINCÍPIO DA NECESSIDADE

Neste princípio, também relacionado ao princípio da finalidade, o objetivo é que as coletas e os tratamentos de dados devem ocorrer minimamente, no que couber para atingir um determinado fim, sendo coletados os estritamente necessários para desempenhar a função a que se propõe.

### 2.3.4. PRINCÍPIO DO LIVRE ACESSO

Trata-se de um princípio vinculado à transparência para o titular de dados a respeito das suas informações coletadas, as quais estão sob tutela do controlador. Em razão disso, é gerada a obrigação de livre acesso às informações do titular para avaliação se está ocorrendo de forma correta, não sendo permitidos que os mesmos sejam manipulados ou excluídos de forma arbitrária pelo controlador.

### 2.3.5. PRINCÍPIO DA QUALIDADE DOS DADOS

A partir do consentimento do titular de dados, é preciso que as informações estejam atualizadas, claras e exatas para não contenha imprecisões a fim de que se tenha qualidade dos dados. Nessa perspectiva, Rony Vainzof afirma:

Qualquer imprecisão, seja um dado pessoal equivocado, seja desatualizado, pode ser catastrófico ao titular, como ocasionar um erro de tratamento médico, recusa de crédito, vedação de participação em concursos públicos, eliminação em processo seletivo, ou, até mesmo, uma prisão injusta (MALDONADO e BLUM, 2019, p. 149).

Nesse viés, conforme afirmado pelo autor, a imprecisão dos dados pode ser prejudicial ao titular, tornando responsável o controlador tomar medidas que mantenham a integridade desses dados.

#### 2.3.6. PRINCÍPIO DA TRANSPARÊNCIA

Este é um princípio que, ausente, inviabiliza toda a efetividade da lei. Para que se tenha uma norma que trate da proteção de dados, a transparência se torna essencial em todo o processo, sendo necessário ser observado desde antes do fornecimento do consentimento, por parte do titular.

Deve o titular estar ciente sobre os termos da coleta, a finalidade, tratamento, requisitos e, até, o processamento e descarte dos dados de forma clara.

O titular dos dados carece de ampla informação sobre o tratamento dos seus dados para que consiga enxergar, cristalinamente, a legalidade, a legitimidade e a segurança do tratamento de acordo com o seu propósito, adequação e necessidade. Assim, terá condições para refletir sobre o tratamento e tomar decisões de acordo com os seus direitos. A transparência deve ser diretamente proporcional ao poder do tratamento dos dados pessoais (qualitativo e quantitativo) e à capacidade de assimilação dos titulares dos novos e dinâmicos produtos e serviços apresentados para o seu uso (MALDONADO e BLUM, 2019, p. 150).

#### 2.3.7. PRINCÍPIO DA SEGURANÇA

É redundante tratarmos, mas é imprescindível a observância da segurança, uma vez que se tem a garantia de aplicabilidade em todos os meios possíveis para manter a segurança dos dados.

Sendo de responsabilidade dos agentes de tratamento de dados oferecer ao titular um aparato técnico que possibilite evitar acessos não autorizados e, principalmente, vazamento de dados, onde a culpa não será presumida, mas oriunda de verificação técnica daquela violação.

#### 2.3.8. PRINCÍPIO DA RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

Enquanto o princípio da transparência é essencial para a efetivação dos demais, o princípio da responsabilização e prestação de contas remete às consequências do descumprimento da norma. Ou seja, o tratamento é lícito e

regular a partir do momento que atende aos ditames legais, caso contrário, haverá responsabilização.

Prever a responsabilização e a prestação de contas como princípio demonstra a intenção da Lei em alertar os controladores e os operadores de que são eles os responsáveis pelo fiel cumprimento de todas as exigências legais para garantir todos os objetivos, fundamentos e demais princípios nela estabelecidos. E não basta somente pretender cumprir a Lei, é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes. Ou seja, os agentes deverão, durante todo ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos (MALDONADO e BLUM, 2019, p. 166-167).

Este princípio demonstra a importância central quanto ao disciplinamento do tratamento de dados, uma vez que, a responsabilidade civil se relaciona a função restaurativa e preventiva, cumprindo um papel civilizatório.

#### **2.4. A RELAÇÃO ENTRE A LEI DE ACESSO À INFORMAÇÃO E A LGPD**

A Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados tem como condão regulamentar o direito constitucional dos cidadãos de acesso à informações, de forma a reforçar a transparência pública e intensificar o processo de legitimação democrática. É importante frisar que existem pontos nos quais as legislações convergem e outros que divergem, mas para compreender devem ser analisados alguns pontos.

Isto posto, os direitos fundamentais tutelados por ambas as leis estão previstos em Constituição Federal, sendo o direito a informações públicas e direito à proteção de dados pessoais (incluindo por meios digitais), nos incisos XXXIII e LXXIX do art. 5º, respectivamente.

Nesse íterim, o direito à informação segue premissas fundamentais, devendo ser desburocratizado o acesso à informação e sem limitações. Por isso, a LAI trata foi construída tendo a publicidade como regra e o sigilo como exceção (inciso I do art. 3º da LAI), sendo as informações de interesse público devendo ser divulgadas independente de uma solicitação.

Em contrapartida, o direito à proteção de dados pessoais, como o próprio nome sugere, busca “proteger os direitos fundamentais de liberdade e de

privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º da LGPD), impondo desde então limitações entre a proteção de dados e privacidade quanto ao acesso a informações. Diante disso, com o passar do tempo a proteção de dados ganha proporções mais autônomas e a privacidade se mantém como um de seus pilares, sendo reconhecido como um direito fundamental autônomo pela Emenda Constitucional 115/2022.

Ao contrário do que se observa nas negativas de acesso à informação que se baseiam na LGPD, a proteção de dados e o acesso à informação não se encontram em pólos distintos uma vez que a proteção de dados se diferencia da proteção à privacidade. Entretanto, o ordenamento jurídico brasileiro conta com parâmetros mais específicos a fim de garantir o acesso a informações de interesse público, para então aumentar a segurança jurídica em sua disponibilização.

Assim, o princípio da publicidade dos atos da Administração permanece intacto e deve ser fomentado pela LAI. As diretrizes estabelecidas pela LGPD estabelecem apenas regras de utilização das informações dos indivíduos, o tratamento desses dados e o direito do cidadão em saber quando seus dados estão sendo captados, saber quais e porque estão sendo coletados.

### **3. A LGPD, COMPLIANCE E GOVERNANÇA NA ADMINISTRAÇÃO PÚBLICA**

A inserção do setor público à LGPD constitui como um marco uma vez que obriga a Administração Pública a investir, se adequar, investir em políticas de segurança e a atuar de forma a evitar o uso desenfreado dos dados pessoais cuja finalidade seja divergente daqueles para os quais foram coletados (LACET, 2020). Desse modo, a redação legislativa estabelece regras específicas para o tratamento de dados pelo Poder Público, devendo este fornecer informações claras e atualizadas a respeito para qual fim está atrelada à necessidade do tratamento de dados em questão e a obrigação de indicar um encarregado, nos termos do artigo 39 da Lei.

Segundo a mesma procuradora (2019), a captação e retenção de dados pessoais pelo setor público é uma atividade essencial para o desenvolvimento de políticas públicas. Por isso, para que ocorra a implementação das regras de conformidade da LGPD no setor público, faz-se necessário o investimento em três pilares: a tecnologia, de modo a fortalecer a política de segurança em TI, em

especial as aplicações que tratam dos dados pessoais; processos, a fim de mapeá-los para compreender o fluxo de tratamento de dados e identificar quais seriam os riscos inerentes a tratamento; e pessoas, para que sejam capacitadas e tenham consciência da importância em estar e permanecer em conformidade com a lei.

Um dos maiores obstáculos da Administração Pública está no compartilhamento dos dados pessoais sem prejudicar a proteção e a segurança das informações, desde a coleta até a sua destruição. Vale ressaltar que o compartilhamento de dados pelo Poder Público e entidades privadas é vedado, exceto nos casos de execução descentralizada de atividade pública para finalidade específica e determinada, com previsão em convênios, contratos e instrumentos congêneres.

Tendo em vista a complexidade e responsabilidade no tocante ao tratamento de dados, a partir da vigência da LGPD, é indispensável que a Administração Pública deva, mais do que nunca, implementar e assegurar o *Compliance* Público, de modo que seja indispensável no mapeamento do fluxo do tratamento de dados e identificação de potenciais riscos no processo de tratamento, uma vez que detém o direito dotado de fé pública.

Para isso, o *compliance*, enquanto instrumento de governança pública, tem o objetivo de atender a legislação vigente mantendo o órgão ou entidade em conformidade às normas de ordenamento jurídico brasileiro.

### 3.2. BOA GOVERNANÇA

A partir da governança corporativa, que é definida como um conjunto de práticas que objetivam regular a administração pública e o controle das instituições, originou-se a ideia da governança pública. Conforme conceitua o Decreto 9.203/2017 no inciso I do art. 2º, a governança pública é composta por um conjunto de mecanismos de liderança, estratégia e controle de postos em prática a fim de que seja avaliado, direcionado e monitorada a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.

Em suma, a governança pública compreende todas as ações de uma instituição pública a fim de assegurar que sua atuação esteja condizente aos

interesses da sociedade. Conforme estabelecido no Decreto, os princípios que orientam a governança pública são o da capacidade de resposta, integridade, confiabilidade, melhoria regulatória, prestação de contas, responsabilidade e transparência, baseando-se nas seguintes diretrizes:

Art. 19. Os órgãos e as entidades da administração direta, autárquica e fundacional instituirão programa de integridade, com o objetivo de promover a adoção de medidas e ações institucionais destinadas à prevenção, à detecção, à punição e à remediação de fraudes e atos de corrupção, estruturado nos seguintes eixos: I - comprometimento e apoio da alta administração; II - existência de unidade responsável pela implementação no órgão ou na entidade; III - análise, avaliação e gestão dos riscos associados ao tema da integridade; e IV - monitoramento contínuo dos atributos do programa de integridade.

Faz-se necessário compreender as razões pelas quais levaram ao desenvolvimento de uma política específica de orientação à governança pública a fim de proporcionar uma boa condução dessa política, podendo serem elencadas motivações como (i) a necessidade de fortalecimento da confiança do cidadão na gestão estatal; (ii) a busca por uma melhor gerência e iniciativas que provoquem o aprimoramento gerencial; e, (iii) a utilidade de se estabelecer uma escala mínima de segurança pela governança pública.

Uma questão de extrema relevância, gerada pela inobservância das práticas de governança, é a perda de confiança da sociedade na instituição, uma vez que a atuação pública deslegitimada tende a gerar regras com alto custo para sua implementação causando desconfiança por parte da sociedade. Corroborando assim, no aumento da burocracia e da desconformidade.

Para que haja o rompimento desse ciclo de ineficiência e resgate da confiança dos cidadãos é de fundamental importância que se alcance resultados econômicos e segurança, porém essas questões só serão viáveis a partir do momento da adoção de práticas de governança. Portanto, garantir que a atuação pública seja tida como legítima pelo cidadão, de forma a fortalecer o cumprimento voluntário de regras sociais e a reduzir a necessidade de controles mais rídicos e burocráticos é um dos papéis principais da política de governança.

Sendo assim, para se alcançar a boa governança são necessários pilares como transparência, integridade, equidade, responsabilidade dos gestores e prestação de contas, como já tratado anteriormente.

### 3.3. COMPLIANCE

As notícias referentes a vazamento de dados por parte de grandes corporações, assim como os escândalos de corrupção intensificam a busca por empresas éticas, confiáveis e transparentes quanto às suas ações e seguras no uso e retenção de informações pessoais. No cenário brasileiro não é novidade que o Estado não consegue acompanhar as condutas fraudulentas e criminosas rotineiras, frente aos inúmeros escândalos de corrupção, fez com que surgisse a necessidade do uso de mecanismos de direito privado que auxiliassem no combate à fraude e à corrupção. Por isso é de grande importância a implementação do programa de *compliance* digital nas organizações públicas para a proteção de dados em conformidade com a LGPD brasileira, objeto deste estudo.

Os programas de *compliance* tem relação com a fixação de controles internos em reforço à regulação estatal, mantendo a entidade pública em conformidade com suas políticas. Segundo Souza, Maciel-Lima e Lupi afirmam que:

O *compliance* surge com o contorno disciplinar e de se fazer cumprir normas legais, sejam políticas, de empresa privada, de instituição ou órgão público. Surge também com o objetivo de evitar, detectar e, como antídoto a qualquer desvio ou inconformidade que possa ocorrer.

Nessa perspectiva, os programas de *compliance* são importantes instrumentos de governança corporativa também aplicáveis ao setor público, pois traduzem ações sistêmicas com o objetivo de atender ao cumprimento das disposições da legislação vigente, possibilitando a prevenção ou minoração de atos ilícitos e a devida sanção de seus responsáveis. A administração Pública deve ser exemplo de boa-fé, legalidade e boa governança, sendo disposto no art. 37 da Constituição Federal os princípios regentes da Administração, tais como legalidade, impessoalidade, moralidade, publicidade e eficiência, além de outros como ética,

transparência e integridade. Portanto, esses princípios devem ser pautados para a atuação do Estado, inclusive no tratamento de dados.

Na Administração Pública, o *compliance* vem de encontro a necessidade e a importância dos três últimos princípios elencados, sendo uma linha mestre entre o administrador, sua função, conduta, leis e princípios os quais devem ser seguidos tendo como primazia a sociedade. Por não se limitar ao simples cumprimento de regras, mas também a prevenção de demandas judiciais, disseminação da cultura da organização, prevenção da corrupção, evita a manipulação do uso de dados e informações privilegiadas. Dessa forma, promove uma nova cultura para o ambiente que é aplicado e o comprometimento dos indivíduos envolvidos, e no caso da LGPD, uma cultura de cuidado com os dados pessoais dos cidadãos.

Uma das vantagens dos programas de *compliance* é permitir a adequação da gestão de risco da atividade e a prevenção de ilícitos, para que sejam identificados de forma rápida e assertiva descumprimentos e a remediação dos danos decorrentes e o fomento à criação de uma cultura de observância às normas legais e internas. Para a efetiva materialização dessas vantagens, é necessário a existência de instrumentos normativos sendo requisitos mínimos para a efetividade dos programas de *compliance*, sendo o principal deles a avaliação dos riscos da atividade.

Sob essa perspectiva, é necessário identificar os pontos de vulnerabilidade a que a Administração está submetida. Isso permitirá as áreas de exposição para que sejam tomadas medidas preventivas proporcionais aos riscos mapeados. Além disso, devem ser elaborados códigos de conduta, para que haja orientação de quase os comportamentos são aceitos ou vedados, quais são os valores e princípios da entidade e é destinado a todos os envolvidos, inclusive terceiros. Então, é necessária a criação de uma cultura de respeito à ética e às leis, uma cultura de *compliance*.

No tocante a LGPD, podem ser elencados três fatores que fortalecem os mecanismos de *compliance*. O primeiro deles, em decorrência ao escopo de incidência da LGPD, se faz necessária a adaptação de atividades de coleta e tratamento de dados e de qualquer outra operação que utilize informações relacionadas a pessoas naturais. Em seguida, temos o fator associado ao primeiro, a estipulação e enquadramento de níveis de exigência distintos e adaptações para o tratamento dos dados envolvidos, com o objetivo de evitar que a proteção acabe

inviabilizando algumas atividades. O terceiro e último fator consiste na necessidade de conferir a concretude à alguns preceitos empregados pela LGPD para que sejam adotados comportamentos em conformidade com a norma.

É a partir da vigência da LGPD que a interligação entre os fundamentos preconizados na lei e o *Compliance* se tornam evidentes e indissociáveis. A fim de efetivar o cumprimento da LGPD, a Administração Pública deverá implementar e assegurar a continuidade do *Compliance* Público, sobretudo em razão do mapeamento do fluxo do tratamento de dados e identificação de potenciais riscos no processo de tratamento. A LGPD constitui-se, pois, como nova fase do *compliance*.

#### **4. IMPLEMENTAÇÃO DA BOA GOVERNANÇA**

Para a efetiva implantação das políticas de integridade e amadurecimento da cultura de proteção aos dados pessoais, algumas ações são imprescindíveis a serem consideradas, quais sejam: os órgãos públicos devem buscar a constante capacitação das pessoas para atuarem como encarregados; formular os relatórios de impactos, mapear o fluxo de dados de seus sistemas: por onde trafegam, como são armazenados e compartilhados os dados, avaliando quais mudanças devem ser realizadas nesses procedimentos.

Além disso, as avaliações provenientes do mapeamento de dados têm por objetivo proporcionar informações úteis à formulação dos relatórios de impacto e planejar ações preventivas. Assim, o setor público é o maior detentor de dados pessoais, muitos deles de natureza sensível, sobrecarregam os sistemas de dados com informações desnecessárias e desatualizadas.

Em 2019 o Instituto Rui Barbosa lançou as Normas Brasileiras de Auditoria no Serviço Público (NBASP) 4000, com o objetivo de constituir importante instrumento de melhoria do controle e da gestão pública. Os princípios e normas instituídos vão de encontro às boas práticas necessárias à governança no tratamento de dados pessoais, uma vez que são os requisitos da objetividade e ética, compreendidos como comportamentos de profissionais íntegros, para garantir os preceitos de segurança e proteção de dados pessoais amparados pela LGPD. Dentro dessa perspectiva, a implantação de um sistema de integridade, atrelados a governança de dados, *compliance* e gestão de riscos são medidas indispensáveis e urgentes que inicialmente se propõe e no qual deve prosseguir.

## 5. CONSIDERAÇÕES FINAIS

Após a exposição de objetivos da lei e proposições e do *compliance* público relaciona-se com questões emblemáticas para que seja alcançado o verdadeiro comprometimento e encorajamento das adversidades encaradas na gestão de dados pelo Poder Público, pode-se concluir que infelizmente a mera existência de instrumentos normativos não garantem a proteção e segurança dos dados pessoais aos quais estamos vulneráveis. Com a acentuada velocidade da evolução digital globalizada elevaram os dados pessoais a uma condição de commodities e com isso, apresentam em si riscos inerentes a sua própria natureza.

Assim, o simples estabelecimento do *compliance* e dos preceitos da LGPD são norteadores em prol da ética, integridade e proteção dos dados pessoais, onde a necessidade e urgência estão além das normas positivadas, devendo envolver e assegurar o comprometimento dos agentes públicos em sua essência.

Estando a temática diretamente relacionada com a efetiva responsabilização dos controladores e operadores do tratamento de dados, é necessário estabelecer parâmetros de efetivo controle e monitoramento no fluxo de dados, devendo ser realizada a identificação e individualização subjetiva no decorrer do tratamento de dados para fins sancionatórios, inclusive do seu efeito pedagógico. É fundamental minimizar os riscos de conformidades pro forma, por meio de metodologias efetivas e inteligentes que produzam efeitos concretos. A aplicação do *compliance* de Dados abarca as mais diversas singularidades de integridade à proteção e segurança dos dados pessoais para o aprimoramento do processo de transformação.

## REFERÊNCIAS

ALEXANDRINO, Marcelo; PAULO, Vicente. **Resumo de Direito Administrativo Descomplicado**. 9ª. ed. REVISTA E ATUALIZADA. ED. MÉTODO. 2017

ALEXY, Robert. Teoria dos Direitos Fundamentais. 1. ed. São Paulo: Malheiros Editores, 2006.

BRASIL. Lei Geral de Proteção de Dados (LGPD). Lei nº 13.709, de 14 de agosto de 2018. Brasília, 2020d. Disponível em:  
[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 03 nov. 2022.

BRASIL. Marco Civil Da Internet. Lei nº 12.965, de 23 de abril de 2014. Brasília, 2018. Disponível em:  
[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 20 fev. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, 2020b. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 22 fev. 2022.

BRASIL. Guia de Boas Práticas – Lei Geral de Proteção de Dados. 2020a. Disponível em:  
<https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd>. Acesso em: 4 out. 2020.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República.

Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em 03 de novembro de 2022.

BRASIL. Casa Civil da Presidência da República. Guia da política de governança pública. Brasília: Casa Civil da Presidência da República, 2018.

BRASIL. Decreto no 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

Disponível em:

[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2017/decreto/D9203.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm) Acesso em: 12 mai. 2023.

BIONI, Bruno Ricardo Proteção de dados pessoais: a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno R.; SILVA, Paula Guedes F.; MARTINS, Pedro Bastos L. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **LAI E LGPD**, Coletânea de Artigos da Pós Graduação em Ouvidoria Pública, ano 2022, v. 1, 15 mar. 2022. Disponível em: [https://revista.cgu.gov.br/Cadernos\\_CGU/article/view/504](https://revista.cgu.gov.br/Cadernos_CGU/article/view/504). Acesso em: 16 maio 2023.

COELHO, A. C. B. A Lei Geral de Proteção de Dados Pessoais Brasileira como meio de efetivação dos direitos da personalidade. João Pessoa: [s.n.], 2019.

Commercial sector: EU-US Privacy Shield. European Commission. Disponível em: [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-usdata-transfers\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-usdata-transfers_en). Acesso em: 11 out 2022

CRISTÓVAM, José Sérgio da Silva; HAHN, Tatiana Meinhart. ADMINISTRAÇÃO PÚBLICA ORIENTADA POR DADOS: governo aberto e infraestrutura nacional de dados abertos. Revista de Direito Administrativo e Gestão Pública, [S. l.], v. 6, n. 1, p. 1-24, 19 ago. 2020. Conselho Nacional de Pesquisa e Pós-Graduação em Direito - CONPEDI. Disponível em:

<http://dx.doi.org/10.26668/indexlawjournals/2526-0073/2020.v6i1.6388>. Acesso em: 11 out 2022

Frank Pasquale apud FRAZÃO, Ana. Fundamentos da Proteção dos Dados Pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 42

FRAZÃO, Ana. Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais. Palestra proferida no Escola Judicial Desembargador Edésio Fernandes, Tribunal de Justiça de Minas Gerais, set. 2019b.

GODINHO, A. M. O fenômeno da constitucionalização: um novo olhar sobre o Direito Civil. Revista Libertas, Janeiro 2013.

16 e 17

LACET, Érika. LGPD e os impactos na Administração Pública. Disponível em: <http://www.impresso.diariodepernambuco.com.br/noticia/cadernos/economia/2019/10/lgpd-e-os-impactos-na-administracao-publica.html> . Acesso em: 03 nov. 2022

LÉVY, Pierre. A conexão Planetária: o mercado, o ciberespaço, a consciência. Traduzido por Maria Lúcia Homem e Ronaldo Entler. São Paulo: Editora 34, 2001

LIMA, José Jerônimo Nogueira de. **LGPD e Administração Pública: Regulação e aplicação**. Dez/2020. Dissertação (Mestrado em Direito Administrativo) - Pontifícia Universidade Católica de São Paulo PUC-SP. São Paulo. 2020

MAGACHO, Bruna Toledo Piza; TRENTO, Melissa. LGPD e compliance na Administração Pública: O Brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? É possível mensurar os impactos das adequações necessárias no setor público? Quais mudanças culturais promover para a manutenção da boa governança? Revista Brasileira de Pesquisa Jurídica, Avaré, v.2, n.2, p. 07-26, maio/ago. 2021. doi: 10.51284/rbpj.02.trento

MALDONADO, V. N.; BLUM, R. O. LGPD: Lei Geral de Proteção de Dados comentada. 1. ed. São Paulo: Revista dos Tribunais, 2019.

MEDAUAR, Odete. Direito Administrativo Moderno. 21. ed. Belo Horizonte: Fórum, 2018.

OLIVEIRA, Vinícius da Silva. **Lei Geral de Proteção de Dados Pessoais e Administração Pública: Administração da Norma**. 2021. Tese (livre-docência) - Curso de Direito da Universidade do Sul de Santa Catarina - UFSC. Tubarão/SC.

PIAIA, Thami Covatti; COSTA, Bárbara Silva; WILLERS, Miriane Maria; Quarta Revolução Industrial e a Proteção do Indivíduo na Sociedade Digital: Desafios para o Direito; **REVISTA PARADIGMA**, Ribeirão Preto/SP, a. XXIV, v. 28, n. 1, p. 122-140, Jan/Abr. 2019. Disponível:  
<https://revistas.unaerp.br/paradigma/article/view/1444/1287> . Acesso em: 27 de setembro de 2022

PINHEIRO, P. P. Proteção de Dados Pessoais: Comentários à Lei nº 13.709/2018. 1. ed. São Paulo: Saraiva Educação, 2018

PEREZ, Marcos Augusto. As Agências Reguladoras no Direito brasileiro: origem, natureza e funções. Revista de Direito Administrativo e Constitucional. Curitiba, ano 2, n. 5 (2000), p. 59-66

SCHRAMM, Fernanda Santos. A responsabilidade de terceiros contratados pela administração pública pelo manuseio dos dados pessoais. *IN: POZZO*, Augusto Neves Dal; MARTINS, Ricardo Marcondes (orgs.). **LGPD & Administração Pública: uma análise ampla dos impactos**. São Paulo: Thomson Reuters Brasil, 2020. p. 789-804.

SOUZA, Sílvia Regina; MACIEL-LIMA, Sandra; LUPI, André Lipp Pinto Basto. Aplicabilidade do compliance na Administração Pública em face ao momento político atual brasileiro. Percurso - ANAIS DO I CONIBADEC (Congresso Ibero-Americano de Direito Empresarial e Cidadania). vol.01, nº.24, Curitiba, 2018.p.14.

